



FORSETI



22 | Derecho, Tecnología y Justicia

Forseti. Revista de Derecho
Lima, DERUP

VOL. 14 NÚM. 22



FORSETI

FORSETI

Revista de Derecho

Vol. 14, N° 22, 2025

© DERUP Editores, Lima, 2025

Av. Gral. Salaverry 2020, Oficina B-302-A Jesús María, Lima, Perú

El contenido de los artículos publicados en FORSETI - Revista de Derecho es responsabilidad exclusiva de los autores.

FORSETI autoriza la reproducción parcial o total del contenido de esta publicación, siempre que se cite la fuente y utilice para fines académicos.

Edición: Setiembre 2025

150 ejemplares

Depósito Legal: 2016-07136

ISSN: 2617-2151 (Impresa)

ISSN: 2312-3583 (En línea)

www.forseti.pe / <https://revistas.up.edu.pe/index.php/forseti/index>

Diagramación:

Mario Popuche

Impreso en Grández Gráficos S.A.C.

Mz. E Lt. 15 Urb. Santa Rosa de Lima - Los Olivos

Setiembre, 2025

Presentación

La Revista *Forseti* tiene el agrado de presentar su edición **número 22**, dedicada al estudio de la compleja relación entre el Derecho, la tecnología y la Justicia. Esta publicación es resultado de un proceso editorial complejo en el que confluyeron aportes de autores y revisores de reconocido prestigio, cuya labor ha permitido consolidar un espacio de reflexión jurídica sobre algunos de los problemas más relevantes de nuestro tiempo.

El eje temático de esta edición responde a la necesidad de examinar, desde una perspectiva crítica, los problemas y desafíos que plantea la implantación y desarrollo de las tecnologías de la información y la comunicación en los distintos ámbitos de la vida institucional y social; especialmente en el mundo jurídico. El contenido ha sido estructurado en tres bloques importantes: i) El Estado y su potestad reguladora en entornos tecnológicos, ii) Los derechos humanos en el contexto tecnológico de nuestro tiempo, y iii) La responsabilidad de las empresas y las organizaciones civiles en la era tecnológica. En esa línea, temas como la incidencia del Big Data en los procesos electorales, la implementación de sistemas expertos en el ámbito judicial o las implicancias jurídicas de la inteligencia artificial son algunas de las cuestiones que aquí se abordan. También se incluyen contribuciones que examinan materias emergentes, tales como los neuroderechos, la protección de datos en contextos tecnológicos, la publicidad digital sustentada en inteligencia artificial o el uso de contratos inteligentes en el mercado inmobiliario.

Este número incluye, además, un apartado de investigaciones de estudiantes, cuyo aporte resulta doblemente valioso: por un lado, porque amplía el espectro de análisis a partir de miradas frescas y originales; y por otro, porque evidencia la formación de nuevas generaciones interesadas en articular el estudio del Derecho con las dinámicas de la transformación digital. Los trabajos que aquí se presentan reflejan un espíritu crítico

frente a problemas tan actuales como los sesgos algorítmicos, las brechas en el acceso a la justicia, la delincuencia potenciada por herramientas de inteligencia artificial y la prevención delictiva basada en modelos predictivos.

El proceso de elaboración de esta edición ha sido exigente, pero profundamente gratificante. Hemos contado con la participación de destacados profesionales nacionales e internacionales, tanto en calidad de autores como de revisores, quienes con su experiencia y rigor académico han contribuido a consolidar la calidad de la revista. A cada uno de ellos, así como al equipo que nos ha acompañado en el proceso editorial, nuestro reconocimiento y agradecimiento.

Con esta nueva edición, *Forseti* cumple, una vez más, su compromiso institucional de difundir investigaciones jurídicas rigurosas e innovadoras, promoviendo un espacio académico con apertura al diálogo interdisciplinario, y que en esta Edición tiene como propósito reflexionar sobre los desafíos que la tecnología plantea al derecho y a la justicia en nuestras sociedades. Estamos convencidas que los artículos aquí reunidos servirán, no solo como material de consulta, sino también como punto de partida para nuevas investigaciones y debates que contribuyan a construir marcos jurídicos más inclusivos, transparentes y acordes con los tiempos que vivimos.

LUCANA M^A ESTÉVEZ MENDOZA
Universidad de Las Palmas de Gran Canaria (España)

MILAGROS OLIVOS CELIS
Universidad del Pacífico (Perú)

Coordinadoras académicas

Coordinación General

Lucana M^a. Estévez Mendoza

Profesora de Derecho Procesal en la Universidad de Las Palmas de Gran Canaria, España. Su trayectoria académica combina la enseñanza y la investigación en campos como la cooperación judicial europea, el espacio de libertad, seguridad y justicia, el terrorismo, la delincuencia juvenil y los nuevos retos que plantean la protección de datos y la inteligencia artificial.

La Dra. Estévez ha consolidado su proyección internacional a través de estancias de docencia e investigación en Hungría, Portugal, Francia y Chile; dimensión internacional que se ve reforzada por su competencia en varios idiomas. Su prestigio ha sido reconocido con su nombramiento como Académica de Número de la Academia de Criminología y Ciencias Forenses de España. Además, ha dirigido tesis doctorales, publicado artículos especializados y participado en proyectos de investigación de alcance nacional e internacional, lo que la consolida como una referente en el ámbito jurídico.

En esta edición especial de FORSETI, su contribución aporta una perspectiva internacional que refuerza el compromiso de la revista con la exigencia académica y un pensamiento jurídico crítico y plural.

Milagros Olivós Celis

Profesora del Departamento Académico de Derecho de la Universidad del Pacífico, Perú desde donde desarrolla labores de enseñanza e investigación en el ámbito del derecho civil, la regulación digital y la protección de datos personales. Realiza su formación doctoral en la Universidad Carlos III de Madrid, con una investigación enfocada en la protección de datos personales en los sistemas de inteligencia artificial.

Su experiencia combina la docencia, la investigación y la práctica profesional en el sector público como privado; enfocando su trabajo en temas de privacidad y regulación digital. En el ámbito académico, ha publicado artículos y capítulos en editoriales de España, Perú y América Latina. Además, participa de seminarios y foros nacionales e internacionales relacionados con la inteligencia artificial, protección de datos y transformación digital en el Derecho.

En esta edición especial de FORSETI, su apoyo fue fundamental para aportar una visión renovada y actualizada sobre los retos que enfrenta la práctica profesional en un entorno globalizado y digital. Su colaboración refuerza la vocación de la revista por tender puentes entre la academia y la práctica profesional, asegurando que el análisis crítico sea complementado con perspectivas útiles para el ejercicio del derecho.

Agradecimientos

La Revista FORSETI desea expresar su más profundo agradecimiento a todas las personas e instituciones que hicieron posible la presente edición especial.

En primer lugar, reconocemos el trabajo constante de la **Comisión de Edición** y de todos los miembros de la Asociación, quienes con dedicación y esfuerzo reafirman en cada número nuestro compromiso con la investigación y el debate jurídico.

Extendemos también nuestro reconocimiento a las coordinadoras generales de esta edición, las profesoras Lucana Estévez Mendoza y Milagros Olivos Celis, cuya orientación académica y acompañamiento fueron fundamentales en la definición de la línea editorial y en la consolidación de este proyecto. Su apoyo es muestra de su valioso perfil académico en tiempo cambiantes para el estudio del Derecho.

Asimismo, agradecemos a los autores que confiaron en FORSETI para difundir sus investigaciones, así como a todos los revisores de pares anónimos, cuya labor rigurosa y silenciosa asegura la excelencia académica de cada artículo publicado.

Nuestro reconocimiento se extiende también a la Facultad de Derecho de la Universidad del Pacífico, liderada por el decano Humberto Zúñiga y todo el personal administrativo que la conforma, por todo el respaldo institucional constante. De manera especial, queremos expresar nuestra más profunda gratitud a la profesoras Jaliya Retamozo Escobar y Rocci Bendezú Barnuevo, cuyo apoyo y acompañamiento académico y logístico fueron decisivos para hacer realidad esta publicación.

Finalmente, agradecemos a nuestros auspiciadores y colaboradores, quienes con su confianza y contribución hicieron posible la materialización de esta edición. A todos ellos, reiteramos nuestro compromiso de seguir construyendo un espacio de diálogo jurídico que combine el rigor académico con la vocación crítica y plural que caracteriza a nuestra revista.

2025-II
Asociación DERUP Editores
Consejo Directivo

Josue Ochoa García
Presidente y Director de Edición

Camila Morales
Vicepresidente

Jeslie Lavado Albino
Acacia Bautista Cervantes
Ana Fernanda Crisanto Solís
Jennifer Plasencia Silva
Luana Sandoval Gallo
Luciana Moreno Manrique
Priscilla Torres Bobadilla
Fabiana Lazo Rentería

Directora de Eventos
Directora de Comercialización
Directora de Finanzas
Subdirectora de Gestión de Talento
Subdirectora de Eventos
Subdirectora de Edición
Subdirectora de Comercialización
Subdirectora de Finanzas

Asamblea General

Comisión de Comercialización

Fiorella Fulchi Leo
Sol Morachimo Quiroz
Camilo Lechuga Hancco
Mauricio Caqui Arévalo
Rodrigo Carranza Távara
María Gracia Gonzales Fajardo
Vanessa Herrada Olivera
Daniela Lecca Dhaga del Castillo
Belén López Fonseca
Joaquín Talavera Becerra
Santiago Negrón Sánchez
Daniela Pita Ahumada
Carmen Segura Manayay
Adriana Sacha Granados
Abigail Gallardo Miranda
Francesca Giribaldi Flórez
Jorge Vera Castañeda

Comisión de Gestión de Talento

Diego Valencia Guevara
Arely Seguil Rodríguez
Alberto Hurtado Rosales
Luis Alonso Larrauri Illescas
Diana Paita Hinostroza
Alisson Mijichich Vila
Mariah Guevara García
Guadalupe De la Cruz
Genaro Ríos Díaz

Comisión de Finanzas

Nadir Quivio Jimenez
Kiara Yasmin Ramos Yañe
Leonardo A. Guevara Gallegos
Amy Palacios Loyola
Maria Fernanda Lam Saldarriaga
Oswaldo Mendoza Damián

Comisión de Edición

Débora Graciano Chávez
Carlos Chuquilin Vasquez
Fabricio Neyra Quijandría
Rafaela Valdivieso Calderón
Ronald Abregú Choque
Luciana Olaza La Rosa
Alicia Valdivia Lazarte
Juan José Barriga Salcedo
Ariana Odria Acosta
Santiago Lores Michaels
Marco Baldizon Roa

Comisión de Eventos

Rina Chanco Sucso
Cesia Esparza Polo
Daniela Mañanes Meléndez
Gabriela Ocampos Sifuentes
Xiomara Hinostriza Pariamachi
Giacomo Sanguineti Ravettino
María Cristina Hau Balta
Mirian Diaz Camones
Patricio Velarde Villegas
Arianna Díaz Quispe

Nuestros Exmiembros

Sebastián de la Puente Astudillo
Ernesto Leoncio Cabrera Falcón
José Luis Repetto Deville
Astrid Medianero Bottger
Sebastián Castro León
Mariem Alicia Nava Zegarra
Elvis Renato Ojeda Huerta
Andrés Hundskopf Wendt
Maria Fernanda Silva Tejada
Karla Berenice Cabrejos Soto
Giuliana Lorena Alvarado Demarini
Daniel Andrés Huapaya Noriega
Germán Gómez Gallegos
Álvaro Reyes O'Neill
Luis Alberto Max Ponce Arnillas
Edith Elizabeth Marquina Rojas
Carlos Eduardo Gasco Bardales
Martín Gallardo Garrath
Maria Angela Ortecho Puente
Andrea Limón Bustamante
Andrea Alexandra Jimenez Garay
Yamila Nair Reinides Tréneman
Claudia Liliana J. Arméstar Alzamora
Vanessa Guissela Minaya Dante
Lorena Rocío Alvarado Ortega
Kathya Alessandra Yauri Grados
Elva Pilar Dionicio Mellado
Diego Alfredo Sedano Bardón
Nataly Paredes Saavedra
Carolina Milagros Neyra Sevilla
Lorena Arascelli Yalta Esterripa
Josefina Alessandra Arana Baldeón
Alejandra Cristina Huachaca Barco
Jorge Luis Changanaquí Miranda
Natalia Alejandra Corigliano Gallardo
Victor Manuel Zacarías Azcona
Gonzalo Lanata Zelada
Dora María Escudero Gómez
Andrea del Pilar Tafur Sialer

Rodrigo García Carthy
Ana Isabel Morales Cerón
Ariana Portilla Balcázar
Diego Alberto Quesada Nicoli
Jackie Carazas Cotrina
Jessica Alessandra Alvarado Bautista
María-Alejandra E. Pons Muzzo S.
Moani Meier Álvarez
Daniela Salynova Baldeón Zamora
Raúl Eliseo Sánchez Flores
Pamela Margot Alvarado Mayor
Audrey Fátima G. Barnett Vidaurre
Astrid Noriega Albújar
Shary Valeria Vergara Ayras
Angela Adriana Ascue Del Aguila
Nicolás Jorge Serván Eyzaguirre
Stephanie Torres García
Ana Lucía Taboada Cárdenas
Ricardo Aureliano Anaya Amaya
Nicolás Daichi Yano Tsuha
Santiago Neira Meza
Rafael Elías Repetto
Melanie Brenis Valencia
Mario Paolo Lafranco Santos
Marcelo Silva-Santisteban Fort
Ana Paula Galvez Fernandez
Valeria Cristina Castro Flores
Giancarlo Montoya Urbano
Denisse Mariana Figueroa D'Ugard
Eduardo Nicolás Contreras Mellado
Nicole Betsabe Nalvarte Atencia
Valeria Alejandra Acosta Chia
Jimena María Ayala Mezzich
Dana Lorena Masumura Ynami
Abrielle Belloni Otayza
Jacqueline Rose St. Laurent del Castillo
Victor Alonso Sousa Delgado
Cesar Alexander Gutierrez Tercero
Valeria Camila Moreno Machin

Carol Estefanía Venegas Ruiz
Antonio Sebastián Robles Vargas
María Milene Jayme Mosquera
Ayrton Hernan Carretero Saravia
Paloma Isabel Cotrina Navarro
César Daniel Valdivia Vergara
Maria Claudia Tamayo Grados
Claudia Zambrano Sotero
Oscar Yalta Esterripa
Jesús David Alfaro Armas
Aniuska Elsa Segura Rios

Allison Patricia Saldamando Egoavil
Renata Ximena Figueroa Sebastián
Maryangel Nisiamá Zaki
Hanna Sheyla Paulino Ramos
Ingrid Isabel Mamani Ccallo
Sandro Fabrizio Olivera Garcia
Bernardeth Quijano Rodriguez
Mariana Desiree Loyola Duarte
Nicolás Andrés Ayala Badillo
Maria Estefania Torres Quiroz Lozano
Joel Jaime Lima Quiroz

Índice

Estado y su potestad reguladora en entornos tecnológicos

El creciente uso de tecnologías digitales emergentes en los procedimientos administrativos: Desde las actuaciones administrativas automatizadas hasta la transparencia algorítmica

Adolfo Morán Caveró y Santiago Castillo Pautrat..... 19

El uso de Big Data en los procesos electorales. El sufragio ¿representa la verdadera voluntad popular? Una mirada desde el sistema jurídico argentino

Lucrecia Contardi Gonzáles..... 61

Sistemas expertos en el Poder Judicial de Perú: El caso de Amauta Pro

Gianfranco Mejía Trujillo..... 81

Justicia y algoritmos: Un análisis ético-jurídico de la Ley 31814 sobre inteligencia artificial en el Perú

Blanca Carrasco Delgado..... 99

El derecho a reusar los datos personales ante las entidades del sector público

*Gabriela Bolaños Vainstein, Rosa Espinoza Córdova
y Ana Taboada Cardenas*..... 117

Más allá del reciente cambio de opinión de la Administración Tributaria, ¿cuál es la forma correcta de calificar un servicio como digital para fines del Impuesto a la Renta?

Sussel Landeo Huamán..... 153

¿Árbitros black box? Los límites al uso de la inteligencia artificial generativa en arbitrajes bajo el principio de indelegabilidad de la función arbitral

Danae Ramos Granados..... 173

La economía digital y el derecho a monetizar la información: Un camino posible

Octavio Salazar Mesías..... 201

Los derechos humanos en el contexto tecnológico de nuestro tiempo

Algoritmos opacos y privacidad diferencial: ¿puede haber transparencia sin comprometer la protección?

Juan Delva Benavides y Valeria Mendez Gonzales 227

Del acoso al abuso en el marco de la violencia sexual ejercida en el ciberespacio

Pablo Cortez Alvarez Cier 245

Consideraciones éticas en la implementación de sistemas de inteligencia artificial para la selección y contratación de personal

Juan De los Santos Esteve..... 269

La positivización constitucional de los neuroderechos en el ordenamiento jurídico peruano

Francesco Aspillaga Muñoz..... 289

Responsabilidad de las empresas y las organizaciones civiles en la era tecnológica

Smart contracts y blockchain en la compraventa de inmuebles futuros: ¿el fin de las estafas en la etapa de preventa?

Luis Cabrera Chalán 309

Los activos digitales y su tratamiento jurídico nacional desde la óptica del Derecho Privado

Martin Mayandía Burns y Diego Munares Cutipa 333

Datos sintéticos y publicidad: desafíos legales en el uso de inteligencia artificial en campañas publicitarias

Malena Cárdenas Tello 353

Inteligencia Artificial en la Publicidad digital: desafíos regulatorios y protección del Derecho de los consumidores

Jasmin Rojas Canales y Próspero Martín Cortez 367

Investigaciones estudiantiles

Brechas digitales e inteligencia artificial: retos en el acceso a la justicia <i>Ivan Polo Olivarez</i>	381
Criminalidad en tiempos de ChatGPT: Análisis del uso de la Inteligencia Artificial como agravante penal en el Perú <i>Giacomo Sanguineti Ravettino</i>	395
Los sesgos naturales en la programación algorítmica: desafíos y dificultades para la aplicación de sistemas automatizados en el derecho <i>Gonzalo Villavicencio Rojas y Juan Pavel Valdez-Rondinel</i>	413
Protección de derechos fundamentales frente a nuevas tecnologías: estudio comparado de Chile, México, Colombia, Ecuador, Bolivia y Perú <i>Eduardo Chocano Ravina y Litzzy Obando Guerrero</i>	439
Prevención delictiva basada en inteligencia artificial: Un análisis desde el derecho a la igualdad <i>Camila Parodi Ccoriñaupa</i>	463

El creciente uso de tecnologías digitales emergentes en los procedimientos administrativos: Desde las actuaciones administrativas automatizadas hasta la transparencia algorítmica

Adolfo Antonio Morán Cavello *

Santiago Gabriel Castillo Pautrat**

Resumen. - En el presente artículo se analiza el uso de tecnologías emergentes por parte de la Administración Pública con el fin de facilitar el acceso y uso a sus prestaciones, a través de actuaciones administrativas automatizadas y procedimientos administrativos automatizados (pudiendo hacerse uso de inteligencia artificial).

Palabras clave.- Metaverso – Inteligencia Artificial – Procedimiento Administrativo Automatizado – Transparencia Algorítmica – Actuación Administrativa Automatizada.

Abstract.- This article analyzes the use of emerging technologies by the Public Administration in order to facilitate the access and use of its services to citizens through automated administrative actions and automated administrative procedures (with the possibility of using artificial intelligence).

Keywords.- Metaverse – Artificial Intelligence – Automated Administrative Procedure – Algorithmic Transparency – Automatic Administrative Processing.

* Abogado por la Pontificia Universidad Católica del Perú (PUCP). Candidato a Master of Laws por The University of Manchester. Investigador Asociado del Grupo de Investigación en Innovación y Transversalidad del Derecho Privado de la PUCP (GIT-PRI).

** Abogado por la Universidad de Lima. Maestría en Derecho Administrativo por la Pontificia Universidad Católica del Perú (PUCP). Especialista en Derecho Administrativo, Derecho Sancionador Financiero y Finanzas Sostenibles. Actualmente es Oficial de Proyectos de Finanzas Verdes de World Wildlife Fund (WWF).

I. Introducción

Las nuevas tecnologías digitales están impactando diferentes escenarios de nuestras vidas, de manera cada vez más persistente y activa. Primero cambiamos las llamadas y los correos electrónicos por videollamadas y servicios de mensajería instantánea; para luego comenzar con una paulatina transición a interactuar en espacios virtuales (metaversos) y al auxilio de la inteligencia artificial (en adelante, “IA” o “inteligencia artificial”) en nuestra vida cotidiana, personal y profesional.

No cabe duda de que todas estas innovaciones han facilitado varios aspectos de nuestra vida diaria, reduciendo plazos y costos en el desarrollo de diferentes actividades. Lo mismo en el ámbito profesional, por ejemplo, las videollamadas fueron definitivamente un paliativo efectivo frente al escenario de aislamiento social obligatorio durante la pandemia del Covid-19, que permitieron reemplazar a las reuniones de trabajo presenciales.

Ahora, se comienza a vislumbrar con gran expectativa lo que puede deparar el uso intensivo de los metaversos y de la inteligencia artificial en la actividad empresarial y profesional. Inclusive, en el ejercicio de la profesión legal¹, así como también como parte de la potestad jurisdiccional. De hecho, el presente trabajo de investigación parte de lo que viene sucediendo actualmente en diferentes jurisdicciones con relación al uso de las tecnologías emergentes comentadas.

Así, es importante destacar que diferentes jueces de países de América Latina han venido adoptando estas nuevas tecnologías como parte de su labor jurisdiccional. Por ejemplo, la magistrada María Victoria Quiñones del Tribunal Administrativo del Departamento de Magdalena en

¹ Por ejemplo, actualmente la herramienta digital ChatGPT puede elaborar muy fácilmente contratos comunes como un contrato de compraventa o un contrato de arrendamiento, lo que podría facilitar la labor de un abogado.

Colombia sustentó la realización de una audiencia² en el “metaverso”³ usando para ello la plataforma Horizon Workrooms, la cual se llevó a cabo el 15 de febrero de 2023⁴.

Por otro lado, el juez peruano Frank Paul Flores García del Juzgado Civil Transitorio de San Juan de Miraflores del Distrito Judicial de Lima Sur resolvió un proceso de alimentos utilizando para ello ChatGPT, un *chatbot* que opera mediante un modelo de lenguaje de gran escala⁵ (LLM)⁶ desarrollado por la empresa estadounidense OpenAI.⁷ En este caso, el juez Flores García utilizó ChatGPT para determinar cuál debía ser el aporte que cada padre debía otorgar para la manutención de su hijo según sus condiciones económicas.

² La magistrada Quiñones resolvió el pedido de la parte demandante (Unión Temporal de Servicios Integrados y Especializados de Tránsito y Transporte de Santa Marta - SIETT) para la realización de la audiencia inicial del proceso seguido contra la Policía Nacional de Colombia (parte demandada) en el metaverso. Puede verse el sustento de dicha decisión en el siguiente enlace: <https://forogpp.files.wordpress.com/2023/02/2020-014-siett-vs-nacion-policia-nacional-solicitud-audiencia-en-el-metaverso-1.pdf>

³ El concepto de metaverso aún se encuentra en desarrollo. Este término apareció por primera vez en la novela de ficción *Snow Crash* del escritor estadounidense Neal Stephenson en 1992. Posteriormente, el metaverso se popularizó a lo largo del 2022, a partir de las declaraciones de Mark Zuckerberg sobre las oportunidades que ofrecía el desarrollo de este espacio virtual en conjunto con una experiencia inmersiva, llegando a cambiar el nombre de su compañía a Meta Platforms Inc. Así, hoy en día existen distintos metaversos con diferentes características, tales como, Decentraland y The Sandbox.

⁴ Puede visualizar la grabación de la audiencia en la mencionada plataforma a través del siguiente enlace: https://www.youtube.com/live/LXi2TX9OBmQ?app=desktop&feature=share&fbclid=PAaAYWsM_8oqTNxiMcmufdXGz5lDqDj_9BBc1zCLBovcQIMzljugykjWxAug#bottom-sheet.

⁵ Un modelo de lenguaje a gran escala se refiere a un sistema computacional que ha sido entrenado utilizando ingentes cantidades de datos para - principalmente - predecir la probabilidad de que una serie de palabras o caracteres aparezcan en una situación en particular a partir de un contexto precedente (SÁNCHEZ & Gasser, 2021; GUTIÉRREZ, 2023b).

⁶ Por sus siglas en inglés: Large Language Model.

⁷ La sentencia puede verse en el siguiente enlace: <https://img.lpderecho.pe/wp-content/uploads/2023/03/Expediente-00052-2022-18-3002-JP-FC-01-LPDerecho.pdf>

Al respecto, han surgido voces a favor y en contra del uso de estas tecnologías emergentes en la labor jurisdiccional⁸, algunos incluso señalando que no se pueden utilizar porque la norma no lo permite o no está preparada⁹.

Sin embargo, consideramos que el análisis jurídico del uso de tecnologías digitales emergentes en la Administración Pública¹⁰ en el Perú sigue en desarrollo. Ya desde hace un tiempo la Administración Pública viene desarrollando un proceso de transformación digital a todo nivel a partir de la entrada en vigencia de la Ley de Gobierno Digital, aprobada por el Decreto Legislativo N° 1412, y su Reglamento, aprobado por el Decreto Supremo N° 029-2021-PCM.

De esta manera, al día de hoy es posible encontrar procedimientos administrativos automatizados en diferentes instancias administrativas, cuya automatización implica que se relegue o se limite la actuación

⁸ Entre las personas a favor del uso de tecnologías emergentes en la actividad jurisdiccional se encuentra la magistrada María Victoria Quiñones quien manifiesta que “desde un punto de vista procesal, nos dimos cuenta de que la utilización de estas herramientas permite retomar las solemnidades y las ritualidades que son propias de la administración de justicia, teniendo en cuenta que todos los movimientos realizados por la persona, así como su voz, están representados en el avatar” (Quiñones, 2023). Por otro lado, especialistas en derecho digital han criticado el uso de herramientas de inteligencia artificial como ChatGPT en la labor jurisdiccional debido a que pueden arrojar resultados elaborados con información falsa; por lo que sería irresponsable usar estas herramientas sin mayor reflexión o sin contrastar la información utilizada (Toche Vega, 2023; Gutiérrez, 2023a).

⁹ Al respecto, el abogado civilista Mejorada (2023) ha señalado que “la legislación procesal del Perú no está preparada para recibir esta asistencia. Según esta legislación, los jueces solo pueden valerse de órganos de auxilio judicial: peritos, tasadores y otros. Y de auxiliares de justicia: los asistentes, secretarios y demás. No está previsto un recurso a una plataforma de inteligencia artificial”.

¹⁰ Al respecto, véase por ejemplo: (i) HUAPAYA, R. (2019). Reflexiones para el tránsito de una Administración Electrónica hacia una Administración Digital en el ordenamiento público peruano. En D. Z. (coordinador), La proyección del Derecho Administrativo peruano: estudios por el Centenario de la Facultad de Derecho de la PUCP (págs. 43-105). Lima: Palestra; (ii) HUAMÁN, R. d. (2019). La optimización del gobierno electrónico como factor clave de la modernización de gestión pública ante el actual Estado de Emergencia. *Revista de Derecho Administrativo*; Núm. 18 (2019); y, (iii) JIJENA, R. (2016). Gobierno Electrónico, Transformación Tecnológica del Gobierno y Derecho. *Foro Jurídico*; Núm. 15 (2016), 199-213.

de servidores públicos en el desarrollo de una o más etapas del procedimiento administrativo.

A partir de lo dicho, y siguiendo la tendencia del poder judicial, es seguro que cada vez más veamos actuaciones de la Administración Pública que involucren el uso de tecnologías tales como el metaverso y ChatGPT (inteligencia artificial). Por ello, resulta fundamental conocer y entender de antemano en qué consiste un procedimiento administrativo automatizado – que actualmente existe – y cómo la inteligencia artificial puede irrumpir en las actuaciones de Administración Pública, e incluso incorporarse dentro de la fiscalización administrativa.

Dicho esto, las siguientes páginas irán abordando distintos conceptos relacionados con el uso de tecnologías emergentes por parte de la Administración Pública considerando la situación actual en el Perú, en tanto la regulación aplicable y los principales casos de uso.

II. Las tecnologías digitales emergentes en la Administración Pública

Los gobiernos de todo el mundo tienen marcada en sus agendas la transformación digital de la Administración Pública. En el Perú, hoy en día, existen distintos procedimientos administrativos que son automatizados¹¹ mediante el uso de tecnologías emergentes, prescindiendo en una o más etapas de la actuación humana¹².

Ahora bien, resulta necesario clarificar qué involucra la transformación digital de la Administración Pública. Sobre ello, en la actualidad esta transformación digital no solo implica el reemplazo de medios físicos por medios electrónicos (p.ej. de documentos en papel a documentos

¹¹ SORIANO (2022) hace la distinción entre sistemas automatizados e inteligencia artificial. Sobre los sistemas automatizados, indica que “son aquellos en los que el resultado se encuentra previamente determinado y que no disponen de la capacidad de actualizarse ni tomar decisiones de manera autónoma” (Soriano, 2022, p. 13). Por otro lado, define a la inteligencia artificial como “un programa que sea capaz de procesar datos de manera masiva, autónoma como lo haría la mente humana, llegando a conclusiones que se caracterizan por ser generalmente más precisas que aquellas que podrían ser alcanzadas por cualquier persona” (Soriano, 2022, p. 13).

¹² A lo largo de este artículo veremos distintos casos de procedimientos administrativos automatizados.

electrónicos), sino que ésta involucra el uso de las tecnologías de la información y comunicación (TICs) en el desarrollo de las actividades de la Administración Pública, (Martínez, 2009; Huapaya, 2019)^{13 14}.

De acuerdo con Martínez (2009), el uso de las TICs en la Administración Pública puede dividirse en dos (2) dimensiones: (i) la dimensión interna, referida a las actividades de la administración relacionadas con las actividades internas de las entidades públicas y en las relaciones entre estas entidades; y, (ii) la dimensión externa, referida a las relación de la Administración Pública con los administrados, por ejemplo, en los servicios públicos y los procedimientos administrativos.

Al respecto, Cerrillo i Martínez (2016)¹⁵ es claro en definir lo que involucraría una Administración Digital¹⁶:

“La administración digital se refiere al uso de la tecnología no solo para automatizar los procesos de las Administraciones Públicas, sino también para generar valor público. La administración digital va más allá de la administración electrónica. Las nuevas tecnologías móviles, el *cloud computing*, el *big data*, los datos abiertos y la colaboración entre las Administraciones Públicas, la ciudadanía, las empresas y la sociedad civil se unen a los mecanismos e instrumentos propios de la administración electrónica para construir unas Administraciones Públicas abiertas y eficientes que prestan unos servicios personalizados y accesibles a la ciudadanía y a las empresas. De este modo, la administración digital no sólo persigue incrementar la eficacia administrativa, sino también fortalecer la apertura y la transparencia de las Administraciones Públicas y la personalización de los servicios que ofrecen a la ciudadanía y a las empresas a través de la innovación que facilitan las nuevas tecnologías que se van consolidando día a día.”

¹³ MARTÍNEZ, R. (2009). Administración Pública Electrónica. Madrid: Thomson Reuters-Civitas.

¹⁴ HUAPAYA, R. (2019). Reflexiones para el tránsito de una Administración Electrónica hacia una Administración Digital en el ordenamiento público peruano. En D. Z. (coordinador), La proyección del Derecho Administrativo peruano: estudios por el Centenario de la Facultad de Derecho de la PUCP (págs. 43-105). Lima: Palestra.

¹⁵ CERRILLO, A. (2016). A las puertas de la Administración digital: Una guía detallada para la aplicación de las leyes 39/2015 y 40/2015. Madrid: INAP.

¹⁶ En el Perú, el concepto de Gobierno Digital, regulado en el artículo 6 de la Ley de Gobierno Digital, haría referencia al concepto de Administración Digital (HUAPAYA, 2019, p. 49).

Dicho esto, los esfuerzos por conseguir una verdadera Administración Digital a todo nivel se ven materializados en diferentes iniciativas que se llevan a cabo por los gobiernos de todo el mundo, utilizando para ello las tecnologías digitales emergentes disponibles.

Por ejemplo, en la ciudad china de Hangzhou se ha lanzado hace algunos años el proyecto *City Brain*, el cual consiste en el uso de inteligencia artificial para la gestión inteligente del tráfico a partir del análisis de gran cantidad de data recopilada por medio de cámaras de vídeo, semáforos, GPS, etc. De esta manera, por ejemplo, la inteligencia artificial puede decidir desviar el tráfico para liberar una calle o avenida y así agilizar el transporte de una ambulancia (Berryhill, Kok Heang, Clogher, & McBride, 2019, p. 80)¹⁷.

Incluso, el gobierno de Corea del Sur ha anunciado la creación de la ciudad de Seúl en el metaverso (*Metaverse Seoul*). Esta ciudad se crea bajo los valores de libertad, inclusión y conexión con la finalidad de crear un espacio virtual seguro para sus ciudadanos que les permita acceder a servicios públicos, así como efectuar reclamos y pagar impuestos.¹⁸

En el Perú, el Instituto Nacional de la Competencia y la Protección de la Propiedad (INDECOPI) ha implementado el denominado Centro Especial de Monitoreo del Instituto Nacional (CEMI)¹⁹, una herramienta de inteligencia artificial para “la recopilación, procesamiento y evaluación

¹⁷ BERRYHILL, J; KOK HEANG, K; CLOGHER, R & MCBRIDE, K. (2019). Hello, World: Artificial intelligence and its use in the public sector. Paris: OECD Publishing.

¹⁸ Para más información de este proyecto puede visitar el siguiente enlace: <https://english.seoul.go.kr/official-release-of-metaverse-seoul/>.

¹⁹ El INDECOPI (2021), ha señalado lo siguiente sobre el CEMI: Precisamente, el Centro Especial de Monitoreo del Indecopi es una herramienta que, mediante el uso de inteligencia artificial, supervisa el comportamiento del mercado desde el inicio de la emergencia sanitaria, a fin de detectar afectaciones a los derechos de los ciudadanos. Así brinda respuestas rápidas y oportunas a casos sensibles que afectan a la ciudadanía, a través de la activación de fiscalizaciones a empresas y proveedores. A la fecha, ha procesado un total de 250 394 reportes y consultas, lo que no solo facilita la elaboración del diagnóstico de la problemática para enfocar acciones de fiscalización inmediatas en los casos de mayor gravedad y sensibilidad; sino que también, permite trasladar la información a otros actores para la mejor toma de decisiones como: entidades del Estado, gremios empresariales y la propia ciudadanía. (p. 1)

de la información sobre la problemática que afecta a los consumidores durante la adquisición de un producto o servicio” (INDECOPI, 2022). De esta manera, el INDECOPI puede entender mejor las afectaciones a los derechos de los consumidores que ocurren en distintos mercados, actuando de manera más oportuna y con fiscalizaciones más efectivas.

De igual modo, en el año 2023 se promulgó la Ley que promueve el uso de la inteligencia artificial en favor del desarrollo económico y social del país, aprobada por la Ley N° 31814²⁰. Dicha norma incluyó una regulación sobre los principios²¹ aplicables al uso de la inteligencia artificial en el Perú, dentro de los que destacan: (i) estándares de seguridad basados en riesgos; (ii) enfoque de pluralidad de participantes; (iii) gobernanza de internet; (iv) sociedad digital; (v) desarrollo ético; y, (vi) privacidad de la inteligencia artificial. Si bien es cierto que se encuentra pendiente su reglamentación y también el desarrollo de jurisprudencia en materia administrativa, su entrada en vigencia demuestra una inquietud del legislador peruano sobre una temática tan crítica en el mundo como la inteligencia artificial y que además tendrá implicancias para el Derecho Administrativo (debido a su posible aplicación en procedimientos administrativos y actuaciones administrativas).

Como se puede apreciar, estamos viviendo tiempos en los que la transformación digital de la Administración Pública está avanzando a

²⁰ No es el objetivo de este artículo analizar la aplicación de la Ley que promueve el uso de la inteligencia artificial en favor del desarrollo económico y social del país, aprobada por la Ley N° 31814. Su aplicación y análisis de parte de órganos resolutivos de la Administración Pública y el Poder Judicial todavía no ha alcanzado una madurez suficiente para la realización de un estudio adecuado. Sin embargo, advertimos que conviene la realización de un estudio profundo de las instituciones contenidas en dicha norma y que el mejor escenario para un análisis es cuando podamos encontrar una cantidad óptima de resoluciones administrativas y sentencias en las que se hallan utilizado.

²¹ **Artículo único. Principios para el desarrollo y uso de la inteligencia artificial**

Son principios para el desarrollo y uso de la inteligencia artificial:

- a) Estándares de seguridad basados en riesgos
- b) Enfoque de pluralidad de participantes
- c) Gobernanza de internet
- d) Sociedad digital
- e) Desarrollo ético para una inteligencia artificial responsable
- f) Privacidad de la inteligencia artificial

pasos agigantados de la mano de las tecnologías digitales emergentes, lo cual conlleva a reevaluar las normas y procedimientos actualmente aplicables a la Administración Pública a fin de dotar a la misma de la habilitación legal necesaria para una transición segura y eficiente a una Administración Digital.

III. El Procedimiento Administrativo Automatizado

Las Administraciones Públicas han implementado actuaciones automatizadas y procedimientos administrativos automatizados, en el marco del denominado derecho de los administrados a relacionarse electrónicamente con la administración. Este derecho no solo habilita al administrado de tomar la libre decisión de relacionarse con la administración usando medios electrónicos, sino también de decidir la interrupción del uso de estos medios y a utilizar los medios y tramitación de un procedimiento ordinario.

Sobre dicho derecho, Martín (2017) señala lo siguiente:

“Corresponde al ciudadano la opción por los medios electrónicos o por los medios convencionales a la hora de realizar un concreto trámite o seguir un procedimiento. (...) De la misma manera, se le reconoce la posibilidad de revocar en cualquier momento su opción por los medios electrónicos, pasando a medios convencionales. Finalmente, para determinados casos, la Administración puede exigir el uso de medios electrónicos, imponiendo la consecuente obligación al ciudadano por vía reglamentaria.”²²

En el Perú, este derecho ha sido reconocido por el artículo 40²³ del Reglamento de la Ley de Firmas y Certificados Digitales, aprobado por

²² MARTÍN, I. (2017). Capítulo 6. Una panorámica general del impacto de la nueva Ley de Procedimiento Administrativo Común en las relaciones de los ciudadanos con la Administración Pública. En I. Martín (Director), *La reforma de la Administración Electrónica: Una oportunidad para la innovación desde el Derecho*, pp. 159-196. España: Instituto Nacional de Administración Pública.

²³ **Artículo 40.- Del derecho ciudadano de acceso a servicios públicos electrónicos seguros**
El ciudadano tiene derecho al acceso a los servicios públicos a través de medios electrónicos seguros para la realización de transacciones de gobierno electrónico con las entidades de la Administración Pública, como manifestación de su voluntad y en el marco de lo previsto en la Ley del Procedimiento Administrativo General - Ley N° 27444.

el Decreto Supremo N° 052-2008-PCM, y complementado por otros derechos conexos previstos en el artículo 42° del mismo Reglamento. A su vez, corresponde que destaquemos dos (2) derechos conexos que han sido reconocidos en el artículo 42° del Reglamento comentado: (i) el derecho a relacionarse con las entidades de la Administración Pública por medios electrónicos seguros para el ejercicio de todos los derechos y prerrogativas (numeral 1²⁴); y, (ii) el derecho a optar por relacionarse con las entidades de la Administración Pública ya sea empleando los centros de acceso ciudadano o a través de canales seguros para la realización de transacciones de gobierno electrónico que éstas deberán poner a su disposición (numeral 2²⁵). Sobre esta incorporación dentro del ordenamiento peruano, Huapaya (2019)²⁶ indica que “una vez que se establece dicho derecho, nace una correlativa obligación de las entidades de la Administración Pública de implementar los servicios y procedimientos digitales para poder permitir el ejercicio de dicho derecho²⁷” (p. 70).

²⁴ **“Artículo 42.- De los derechos conexos**

El derecho ciudadano de acceso a servicios públicos electrónicos seguros tiene como correlato el reconocimiento de los siguientes derechos:

42.1. A relacionarse con las entidades de la Administración Pública por medios electrónicos seguros para el ejercicio de todos los derechos y prerrogativas (...) En tal sentido, constituye obligación de la Administración Pública facilitar el ejercicio de estos derechos ciudadanos, debiendo promover la prestación de servicios por medios electrónicos. (...)”.

²⁵ **“Artículo 42.- De los derechos conexos**

El derecho ciudadano de acceso a servicios públicos electrónicos seguros tiene como correlato el reconocimiento de los siguientes derechos:

(...)

42.2. A optar por relacionarse con las entidades de la Administración Pública ya sea empleando los centros de acceso ciudadano o a través de canales seguros para la realización de transacciones de gobierno electrónico que éstas deberán poner a su disposición. (...)”.

²⁶ HUAPAYA, R. (2019). Reflexiones para el tránsito de una Administración Electrónica hacia una Administración Digital en el ordenamiento público peruano. En D. Z. (coordinador), *La proyección del Derecho Administrativo peruano: estudios por el Centenario de la Facultad de Derecho de la PUCP* (págs. 43-105). Lima: Palestra.

²⁷ En el caso de España, Martínez (2009) indica que: “La Ley española 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos (en adelante también LAECSP) ha consagrado en su artículo 6° el derecho de los ciudadanos a relacionarse con las administraciones públicas por medios electrónicos. (...) Es decir,

Sobre las actuaciones administrativas automatizadas, Domínguez (2021)²⁸ indica que “son cualquier acto o actuación realizada íntegramente a través de medios electrónicos por una Administración Pública en el marco de un procedimiento administrativo y en la que no haya intervenido de forma directa un empleado público” (pp. 313-314). En el Perú no existe una norma que regule de manera expresa las actuaciones administrativas automatizadas, pero le son aplicables las garantías de la Ley del Procedimiento Administrativo General y de la Ley del Gobierno Digital²⁹ y su Reglamento.

Sin embargo, en España sí encontramos una regulación expresa sobre el tema, el artículo 41³⁰ de la Ley 40/2015, establece requisitos para

configura la posibilidad para los administrados de desarrollar electrónicamente los derechos clásicos reconocidos por la LRJPAC a favor de los ciudadanos, lo que supondrá, lógicamente, que las administraciones deberán disponer de los dispositivos electrónicos o plataformas tecnológicas necesarias para permitir el cumplimiento de este derecho. (...) el artículo 42º del Reglamento de la Ley de Firmas y Certificados Digitales, ya que el mismo se refiere a la materialización de los “derechos conexos” que permitirán el ejercicio del derecho de acceso de los ciudadanos a los servicios públicos, siendo éste el artículo del ordenamiento peruano equivalente al artículo 6º de la LAECSP española (...)”. (pp. 97 - 99)

²⁸ DOMÍNGUEZ, J. (2021). Inteligencia Artificial, derecho administrativo y protección de datos personales. Entre la dignidad de la persona y la eficacia administrativa. *IUS ET SCIENTIA*: Revista electrónica de Derecho y Ciencia, 304-326.

²⁹ Dentro de estas garantías se encuentran los principios rectores de la Ley del Gobierno Digital. Dentro de estos, encontramos a los siguientes: (i) el Principio de Equivalencia Funcional (los administrados tienen los mismos derechos y garantías que en los servicios y/o procedimiento tradicionales); (iii) el Principio de Igualdad de Responsabilidades (las entidades son responsables por los actos realizados por medios electrónicos de la misma forma como son responsables por los emitidos en procedimientos ordinarios); (iii) el Principio de Usabilidad (el diseño de los sistemas informáticos debe de asegurar uso accesible y práctico por parte del administrado); (iv) el Principio de Datos Abiertos por Defectos (existe transparencia sobre los datos, pero sin afectar la protección de los datos personales); entre otros.

³⁰ **Artículo 41. Actuación administrativa automatizada.**

1. Se entiende por actuación administrativa automatizada, cualquier acto o actuación realizada íntegramente a través de medios electrónicos por una Administración Pública en el marco de un procedimiento administrativo y en la que no haya intervenido de forma directa un empleado público.

2. En caso de actuación administrativa automatizada deberá establecerse previamente el órgano u órganos competentes, según los casos, para la definición

la implementación de actuaciones automatizadas por parte de la Administración Pública. Dentro de éstos se encuentran: (i) la designación de un órgano competente para la definición de las especificaciones, programación, mantenimiento, supervisión y control de calidad y auditoría del sistema de información y de su código fuente; y, (ii) la indicación del órgano que debe ser considerado responsable a efectos de impugnación.

Por otro lado, podemos señalar que las actuaciones administrativas automatizadas son en sí mismas un concepto continente que aglomera a: (i) los actos de trámite automatizados (como una resolución administrativa que admite a trámite un procedimiento); (ii) los actos administrativos automatizados (una declaración de la administración que genere efectos en los intereses y derechos de los administrados); (iii) los servicios digitales (que son una prestación que se caracteriza por ser automática, no presencial y que utiliza de manera intensiva las tecnologías digitales para la producción y acceso a datos, y contenidos que generen valor público para los ciudadanos y personas en general³¹); y, (iv) las actuaciones administrativas automatizadas propiamente dichas³² (es decir, aquellas que no forman parte de ninguna de las tres categorías anteriores).

Sobre el acto administrativo automatizado, Martín (2009)³³ señala que “es igual en contenido que un acto administrativo convencional y su única diferencia radica en que existirán determinados actos administrativos que no podrán ser adoptados de manera automatizada” (p. 365). Tal como señala el autor, existen ciertos actos que son difíciles de ser automatizados, como los procedimientos administrativos vinculados a materias ambientales, debido a que requieren una evaluación de equipos

de las especificaciones, programación, mantenimiento, supervisión y control de calidad y, en su caso, auditoría del sistema de información y de su código fuente. Asimismo, se indicará el órgano que debe ser considerado responsable a efectos de impugnación.

³¹ Esta definición es extraída del artículo 3.3 de la Ley del Gobierno Digital.

³² Como el mensaje de conformidad del cumplimiento de requisitos de un procedimiento iniciado por medios electrónicos.

³³ MARTÍN, I. (2009). Naturaleza, concepto y régimen jurídico de la actuación administrativa automatizada. *Revista de administración pública*, pp. 353-386.

técnicos multidisciplinarios (abogados, ingenieros, economistas, sociólogos, entre otros) y el ejercicio de un mayor nivel de discrecionalidad de parte de la autoridad a cargo.

i. Características del procedimiento administrativo automatizado.

Las características del procedimiento administrativo automatizado son las siguientes:

A. Es un procedimiento administrativo electrónico

Un procedimiento administrativo electrónico es simplemente aquel cuya tramitación se realiza de manera parcial o total a través de medios electrónicos. Sin embargo, debemos advertir que no todo procedimiento administrativo electrónico será automatizado, en la medida que el uso de medios electrónicos no implica la automatización de los actos de trámite y de las actuaciones que se llevan a cabo durante la tramitación de un procedimiento. A pesar de lo anterior, todo procedimiento administrativo automatizado es un procedimiento administrativo electrónico.

En base a esta característica, le son aplicables las garantías del artículo 29-A³⁴ de la Ley del Procedimiento Administrativo General.

³⁴ Artículo 29-A.- Procedimiento Administrativo Electrónico

29-A.1 Sin perjuicio del uso de medios físicos tradicionales, el procedimiento administrativo podrá realizarse total o parcialmente a través de tecnologías y medios electrónicos, debiendo constar en un expediente, escrito electrónico, que contenga los documentos presentados por los administrados, por terceros y por otras entidades, así como aquellos documentos remitidos al administrado.

29-A.2 El procedimiento administrativo electrónico deberá respetar todos los principios, derechos y garantías del debido procedimiento previstos en la presente Ley, sin que se afecte el derecho de defensa ni la igualdad de las partes, debiendo prever las medidas pertinentes cuando el administrado no tenga acceso a medios electrónicos.

29-A.3 Los actos administrativos realizados a través del medio electrónico, poseen la misma validez y eficacia jurídica que los actos realizados por medios físicos tradicionales. Las firmas digitales y documentos generados y procesados a través de tecnologías y medios electrónicos, siguiendo los procedimientos definidos por la autoridad administrativa, tendrán la misma validez legal que los documentos manuscritos.

29-A.4 Mediante Decreto Supremo, refrendado por la Presidencia del Consejo de

Es decir: (i) sus actuaciones deberán constar en un expediente electrónico; (ii) el procedimiento deberá respetar todos los principios, derechos y garantías del debido procedimiento previstos en la Ley del Procedimiento Administrativo General; y, (iii) que los actos administrativos poseen la misma validez y eficacia jurídica que los actos realizados por medios físicos tradicionales.

B. Es un procedimiento realizado por medio de sistemas automatizados

En definitiva, esta característica es central debido a que el procedimiento automatizado implica una limitación y/o eliminación de la participación humana dentro de la tramitación del procedimiento, debido a que es reemplazada por un sistema informático que ejecuta algoritmos diseñados para emitir actos de trámite y actuaciones materiales. Para estos efectos, los desarrolladores del programa informático han realizado un ejercicio previo de parametrización de los actos de trámite y actuaciones materiales que forman parte del procedimiento, generando modelos de respuesta preestablecidos (p.ej. la presentación de los requisitos para el inicio del procedimiento).

Sobre el particular, Martín (2009) indica lo siguiente:

La máquina, la herramienta informática, no deja de ser un medio material, como tantos otros, al servicio del titular del órgano. La diferencia en este caso radica en que el medio material no se limita simplemente a ayudar al titular del órgano a adoptar una decisión en el ejercicio de sus funciones, sino que procede directamente a adoptar la decisión, sin intervención alguna del titular en ese caso concreto. La conexión entre el producto decisional automatizado y el titular del órgano tiene lugar a través de la entrada en juego de la firma electrónica.³⁵

Ministros, se aprueban lineamientos para establecer las condiciones y uso de las tecnologías y medios electrónicos en los procedimientos administrativos, junto a sus requisitos.

³⁵ MARTÍN, I. (2009). Naturaleza, concepto y régimen jurídico de la actuación administrativa automatizada. *Revista de administración pública*, pp. 353-386.

C. Debe ser emitido por un órgano de la administración

La automatización no significa que el sistema sea quien emita el acto. El acto siempre será emitido por un órgano de una entidad, a través del servidor público que tenga la competencia para los efectos de la emisión del acto administrativo. En dicho contexto, el artículo 4.3³⁶ de la Ley del Procedimiento Administrativo General ordena que en el caso de los procedimientos administrativos automatizados se debe identificar plenamente a la entidad que emite el acto y al servidor público a cargo, esto es una garantía de cara a la interposición de recursos impugnatorios (como la apelación o la reconsideración).

Sobre el particular, Martín (2009) indica que “no es sino una forma de adoptar resoluciones administrativas que ni afecta al órgano (que sigue estando integrado por personas físicas y regido por su titular) ni altera la competencia”³⁷. De igual modo, como hemos podido apreciar al comentar la norma española, este aspecto es relevante para asignar responsabilidad sobre la emisión del acto administrativo y para la eventual interposición de mecanismos impugnatorios.

D. Debe existir una habilitación legal

Un procedimiento administrativo regular prevé la participación de servidores públicos, pero un procedimiento automatizado prescinde de dicho elemento, por lo que es necesario que exista una habilitación legal para la automatización.

Sobre el particular, Martín (2009) indica lo siguiente:

“La posibilidad de expresar tal actividad por medios electrónicos, sin intervención de persona alguna, debe estar expresamente prevista y autorizada con carácter previo (...). La norma que habilita para el uso deberá explicitar convenientemente las razones que avalan la posibilidad

³⁶ “Artículo 4.- Forma de los actos administrativos (...)

4.3. Cuando el acto administrativo es producido por medio de sistemas automatizados, debe garantizarse al administrado conocer el nombre y cargo de la autoridad que lo expide. (...)”.

³⁷ MARTÍN, I. (2009). Naturaleza, concepto y régimen jurídico de la actuación administrativa automatizada. *Revista de administración pública*, pp. 353-386.

de automatización del proceso decisor y, además, deberá concretar las exigencias que debe reunir el sistema de información en que la actuación automatizada se basa para satisfacer los requisitos legalmente exigidos para los actos administrativos. Con ello se garantiza el cumplimiento de los principios de legalidad y seguridad jurídica constitucionalmente consagrados.”³⁸

Este requisito no ha sido regulado expresamente en la Ley del Procedimiento Administrativo General; sin embargo, podemos afirmar que es inherente a la implementación de un procedimiento administrativo automatizado, debido a que de manera general la norma prevé siempre la intervención de servidores públicos en la tramitación del procedimiento.

Ahora bien, sobre si esta habilitación legal se debería dar solo por normas con rango de ley o por normas reglamentarias es todavía un debate abierto, pero consideramos que –desde una perspectiva razonable– se debería habilitar la automatización tanto por normas de rango de ley como por normas reglamentarias, a fin de facilitar su implementación, y en el marco del derecho de los administrados a relacionarse electrónicamente con la administración, cumpliendo con un nivel óptimo de transparencia algorítmica, concepto que explicaremos más adelante.

ii. Tipos de procedimientos administrativos automatizados.

Los procedimientos administrativos automatizados pueden diferir en su nivel de automatización. A partir de ello, podemos distinguir tres (3) tipos de procedimientos administrativos automatizados:

A. Procedimiento administrativo con automatización total

Son aquellos en los que se ha logrado una automatización de todas las etapas, actos de trámite y de cualquier otro tipo de actuación administrativa dentro del procedimiento, desde el inicio de su tramitación hasta su conclusión. Es decir, que en estos procedimientos encontramos el mayor grado de automatización que la Administración Pública puede lograr, habiendo eliminado toda participación humana dentro de la tramitación del mismo.

³⁸ *Idem.*

Un ejemplo de este procedimiento es la emisión del Certificado Único Laboral para Jóvenes (CERTIJOVEN), que es un certificado que reúne información de diversas entidades públicas y que es emitido por el Ministerio de Trabajo y Promoción del Empleo (MTPE), que incluye: (i) datos de identidad; (ii) antecedentes policiales; (iii) antecedentes judiciales; (iv) trayectoria educativa; y, (v) experiencia laboral.

El procedimiento inicia cuando el ciudadano accede al portal web del Servicio Nacional del Empleo del Ministerio de Trabajo y Promoción el Empleo y el sistema informático realiza una verificación de identidad. Luego, el sistema genera automáticamente el certificado, esta automatización se encuentra habilitada por el artículo 7³⁹ del Decreto Supremo N° 014-2018-TR, Reglamento del Decreto Legislativo N° 1378, Decreto Legislativo que fortalece y extiende la accesibilidad al Certificado Único Laboral para Jóvenes.

B. Procedimiento administrativo con automatización parcial

Existen procedimientos con actuaciones automatizadas que pueden configurarse en determinadas etapas del procedimiento, pero que

³⁹ Artículo 7.- Proceso de obtención del Certificado Único Laboral para Jóvenes - CERTIJOVEN

7.1 El/la ciudadano/a accede al portal web del Servicio Nacional del Empleo del Ministerio de Trabajo y Promoción el Empleo (www.empleosperu.gob.pe) mediante su documento nacional de identidad (DNI) y completa su registro con la información que le sea solicitada.

7.2. Durante el registro se activa el procedimiento de validación de identidad virtual conforme a lo establecido por el Ministerio de Trabajo y Promoción del Empleo.

7.3. Culminado el proceso de verificación de identidad del/de la solicitante, **se autogenera inmediatamente su primer certificado el cual se aloja en su carpeta de certificados, mediante la cual puede acceder al mismo para descarga y/o impresión.** Asimismo, el sistema habilita su acceso para que pueda generar un nuevo certificado cada vez que lo solicite, con los datos de su Documento Nacional de Identidad (DNI), a través del portal web del Servicio Nacional del Empleo del Ministerio de Trabajo y Promoción del Empleo (www.empleosperu.gob.pe). La generación de un nuevo certificado no está restringida a la vigencia de uno anterior, pudiendo almacenarse los diez últimos certificados en la carpeta del usuario.

7.4. El procedimiento de validación de identidad también puede realizarse mediante canales alternativos que el Ministerio de Trabajo y Promoción del Empleo autorice e implemente. (El resaltado es nuestro)

no se ejecutan en la totalidad de la tramitación, configurándose una automatización parcial.

Un ejemplo de ello es el procedimiento simplificado de restitución de derechos arancelarios, a cargo de la Superintendencia Nacional de Aduanas y de Administración Tributaria (SUNAT). Este es un régimen especial aplicable al *drawback*; es decir, la devolución de derechos arancelarios para productos que serán exportados, en el que un sistema informático estaría encargado de la evaluación de las solicitudes, su procesamiento y finalmente el pago de dichos derechos arancelarios, aprobado por la Resolución SUNAT N° 000183-2020-SUNAT⁴⁰.

En este caso, el sistema informático revisa los datos de la solicitud (es decir, los detalles de los productos que serán exportados). Más adelante, el sistema determina tres (3) resultados: (i) aprobar la solicitud; (ii) ordenar una revisión documentaria (es decir, que un funcionario revise la información detallada por el administrado); o, (iii) denegar la solicitud y ordenar la subsanación de la misma. Luego de ello, en el supuesto que se apruebe la solicitud o la revisión sea favorable, el sistema ordena al Banco de la Nación a realizar el pago del derecho solicitado.

⁴⁰ “(...) VII. DESCRIPCIÓN

A) DE LA SOLICITUD

1. La voluntad de acogerse a la restitución debe constar en la declaración de exportación regularizada, con la consignación del código N° 13 a nivel de cada serie, en la:

(...)

5. El sistema informático valida los datos de la información ingresada. De ser conforme, genera el número de la solicitud, determina la selección a revisión documentaria o aprobación automática y la notifica a través del buzón electrónico del beneficiario.

(...)

6. De no ser conforme la información registrada, el sistema informático muestra en línea las inconsistencias mediante las alertas respectivas y la solicitud es guardada automáticamente en la bandeja de “solicitudes pendientes de numerar”.

7. Si la solicitud es seleccionada a aprobación automática, se continúa con el proceso automático de verificación de deudas, sin perjuicio de las acciones de fiscalización especial. (...)”.

C. Procedimiento administrativo con un inicio automatizado

Por otro lado, existe otro grupo de procedimientos que se caracterizan en que tan solo su inicio es automatizado. Dicha automatización se concretiza en una evaluación automática, pero preliminar de los requisitos de admisibilidad de la solicitud del inicio del procedimiento. Ahora bien, dicha automatización no significa una automatización de los demás actos, actuaciones y otros, pero sí una facilidad en el inicio del trámite. Así, en una etapa posterior, el servidor público a cargo de la tramitación del procedimiento revisará los requisitos de admisibilidad y realizará y/o emitirá las actuaciones materiales, actos de trámite y el eventual acto administrativo a través de medios convencionales.

Un ejemplo de ello son los procedimientos administrativos del Registro Nacional de Producción y Reaprovechamiento de Biosólidos a cargo del Ministerio de Vivienda y Saneamiento, en el que se ha habilitado la presentación de solicitudes a través un aplicativo virtual, de acuerdo a la primera disposición complementaria final⁴¹ de la Resolución Ministerial N° 300-2017-VIVIENDA. Este sistema informático emite alertas de conformidad sobre el cumplimiento de requisitos para solicitudes para el inicio del trámite de procedimientos administrados vinculados al Registro Nacional de Producción y Reaprovechamiento de Biosólidos. Sin embargo, esta evaluación automatizada no significa la admisibilidad de la solicitud, por lo que también existirá en este procedimiento un acto de trámite elaborado por un funcionario público en el que se

⁴¹ “PRIMERA.- Implementación progresiva del aplicativo virtual

En un plazo no mayor de sesenta (60) días hábiles, contados a partir del día siguiente de publicada la presente Resolución Ministerial en el diario oficial El Peruano, la Dirección General de Asuntos Ambientales del Ministerio de Vivienda, Construcción y Saneamiento implementa en su integridad el aplicativo virtual para la tramitación de los procedimientos administrativos del Registro Nacional de Producción y Reaprovechamiento de Biosólidos.

(...)

Una vez implementado en su integridad el aplicativo virtual, los administrados pueden acceder a los procedimientos administrativos relacionados con el Registro Nacional de Producción y Reaprovechamiento de Biosólidos desde la presentación de su solicitud hasta la conclusión del procedimiento administrativo. Sin perjuicio del uso de medios físicos tradicionales”.

evaluará el cumplimiento de los requisitos para el inicio del trámite del procedimiento.

IV. Sobre la transparencia algorítmica.

La intervención de herramientas digitales y de inteligencia artificial en los procedimientos administrativos va de la mano con un concepto que ha sido desarrollado recientemente por la doctrina⁴² y las Administraciones Públicas de otros países⁴³: la transparencia algorítmica⁴⁴. La transparencia algorítmica es el nivel de publicidad activa o pasiva sobre

⁴² Al respecto, véase por ejemplo: (i) VESTRI, G. (2021). La inteligencia artificial ante el desafío de la transparencia algorítmica. Una aproximación desde la perspectiva jurídico-administrativa. *Revista Aragonesa de Administración Pública*, 368-398; (ii) Hayes, P., de Poel, I. v., & Marc, S. (2022). Moral transparency of and concerning algorithmic tools. En J. MacIntyre, & L. Medsker, *AI and Ethics* (2022); y, (iii) Araya, C. (2020). *Transparencia algorítmica ¿un problema normativo o tecnológico?* Santiago. Obtenido de https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S2452-610X2021000200306.

⁴³ Por ejemplo, la Ley 1/2022, de 13 de abril, de Transparencia y Buen Gobierno de la Comunitat Valenciana ha incorporado un estándar de transparencia algorítmica en los siguientes términos:

“Artículo 16. Información de relevancia jurídica.

1. Las administraciones públicas del artículo 3.2 deben publicar:

(...) 1) La relación de sistemas algorítmicos o de inteligencia artificial que tengan impacto en los procedimientos administrativos o la prestación de los servicios públicos con la descripción de manera comprensible de su diseño y funcionamiento, el nivel de riesgo que implican y el punto de contacto al que poder dirigirse en cada caso, de acuerdo con los principios de transparencia y explicabilidad. (...)”.

A su vez, el Reino Unido ha implementado un reporte periódico y voluntario de transparencia algorítmica de las herramientas de inteligencia artificial que utilizan sus entidades públicas.

⁴⁴ El Cabinet Office (2022) del Reino Unido ha indicado que la transparencia algorítmica favorece tanto al gobierno, al público y a los proveedores externos de la siguiente manera:

For the government, enables government departments to build public trust, highlight good practice, identify problems early on and learn from one another. For the public, algorithmic transparency fulfils the democratic right to information and explanation about how the government makes decisions. For the external suppliers, it helps demonstrate their commitment to ethical service delivery, showcase their value proposition, and improve public trust in their systems (p. 1).

las condiciones de uso, mantenimiento y vulnerabilidades de los *softwares* que sean utilizados en alguna actuación automatizada o procedimiento administrativo automatizado. Es decir, este concepto implica todo lo relativo a las acciones y medios que debería realizar la Administración Pública para compartir con el administrado cómo funcionan los algoritmos⁴⁵ de sus sistemas informáticos, plataformas, herramientas y demás, con la finalidad de asegurar el principio de transparencia⁴⁶ y derechos fundamentales vinculados a entornos digitales, tales como: (i) el derecho a la información; y, (ii) el derecho a la defensa de los administrados.

Así, el desarrollo de mecanismos de transparencia algorítmica implica las acciones que debería realizar el estado para resguardar derechos fundamentales en el nuevo entorno digital. Esto contribuye a la legitimidad de las prestaciones que realiza el estado con la ayuda de las nuevas tecnologías, lo que en el mundo anglosajón se denomina *public trust*. El derecho a la información es fundamental para facilitar la rendición de cuentas que deben realizar los servidores públicos respecto a la ejecución de sus funciones y tareas con recursos públicos. Asimismo, el derecho a la defensa es clave en este entorno para asegurar que el administrado pueda obtener los medios adecuados para salvaguardar sus derechos fundamentales en el hipotético caso de algún daño o riesgo de daño.

⁴⁵ HAYES, DE POEL, & MARC (2022), definen al algoritmo de la siguiente manera: "An algorithm can be defined as a finite set of steps that are carried out to solve a problem (...) They are however often embedded in software tools and computational systems" (p. 1).

⁴⁶ COTINO (2017), indica lo siguiente sobre el principio de transparencia: "La transparencia incluye la información activa, el deber de la administración de dar activamente información de relevancia o interés público", p. 403.

En esta línea, Vestri (2021)⁴⁷ indica lo siguiente sobre la transparencia algorítmica:

(...) en nuestra opinión, es necesario mirar la transparencia de forma bifocal. Por un lado, se hace patente la necesidad de verificar que la elección del algoritmo por parte de la Administración pública sea transparente. En segundo lugar, verificar la transparencia del algoritmo cuando éste se encuentre funcionando en la Administración pública, garantizando la accesibilidad del interesado a conocer cómo el algoritmo adopta la decisión. (p. 393)

La transparencia algorítmica se puede promover a través de mecanismos activos como mecanismos pasivos. Dentro de los mecanismos activos podemos encontrar la publicación de: (i) reportes periódicos; (ii) manuales de uso; y, (iii) documentos con la descripción de especificaciones técnicas, que expresen un nivel óptimo y suficiente de información acerca de las herramientas digitales utilizadas en actuaciones automatizadas y procedimientos administrativos automatizados. Dentro de los mecanismos pasivos hallamos la atención de solicitudes de información de los administrados sobre el funcionamiento de estas herramientas digitales, las que se dan a pedido de parte como parte de un procedimiento reglado (que puede ser el tradicional procedimiento de acceso a la información pública) y con las garantías propias del derecho a la información y del Derecho Administrativo Común.

Adicionalmente, debemos indicar que el nivel de transparencia algorítmica dependerá no solo de las normas legales o buenas prácticas que implementen las entidades públicas, sino también de los términos y condiciones de uso pactados entre la Administración Pública y la empresa o persona desarrolladora del *software*, debido a que los términos y condiciones de la publicidad de sus códigos fuente y/o sus documentos técnicos pueden estar protegidos por los derechos de autor y el secreto comercial (o también denominado secreto empresarial). En esta línea, debemos de advertir que en el Perú los *softwares* están protegidos por la Ley sobre el Derecho de Autor, aprobada por el Decreto Legislativo N° 822, y cuentan con el mismo tratamiento que

⁴⁷ VESTRI, G. (2021). La inteligencia artificial ante el desafío de la transparencia algorítmica. Una aproximación desde la perspectiva jurídico-administrativa. Revista Aragonesa de Administración Pública, pp, 368-398.

una obra literaria, otorgándole una protección a sus derechos morales⁴⁸ y patrimoniales⁴⁹.

Teniendo en cuenta lo anterior, como veremos más adelante, el Consejo de Transparencia y Buen Gobierno de España⁵⁰ (órgano encargado de resolver en última instancia administrativa las solicitudes de acceso a la información pública en el Estado español) ha denegado el acceso

⁴⁸ Sobre los derechos morales, el INDECOPI (2023) indica que son cinco (5):

“¿Cuáles son los derechos morales del autor?

- (i) Paternidad: Es la facultad del autor para determinar si su nombre aparece en la obra, o no (en cuyo caso será una obra anónima); y, si decide que su nombre aparezca, la forma y modo de hacerlo (por ejemplo, su nombre completo o, por el contrario, bajo un seudónimo o un sobrenombre.
- (ii) Divulgación: Es la facultad del autor de decidir cómo, cuándo y dónde difundirá su obra.
- (iii) Integridad: Es la facultad del autor para oponerse a cualquier deformación, mutilación o modificación de su obra.
- (iv) Modificación o variación: Es la facultad del autor para realizar las modificaciones que estime necesarias sobre su obra, o después de su divulgación, sin perjuicio de la indemnización que corresponda, por los daños y perjuicios que genere a los derechos adquiridos por terceros.
- (v) Retiro de la obra del comercio: Es la facultad que tiene el autor para suspender cualquier utilización de su obra, siempre que previamente indemnice a los terceros que puedan verse afectados con el ejercicio de este derecho”, p. 1.

⁴⁹ Sobre los derechos patrimoniales, el INDECOPI (2023) indica que son cuatro (4) y que además incluyen toda forma de utilización o explotación comercial: “¿Cuáles son los derechos patrimoniales del autor?

- (i) Comunicación pública: El autor o titular del mismo es el único que puede autorizar o prohibir la comunicación pública (es decir permitir el acceso a la obra sin previa distribución de ejemplares), de todo o parte, de la obra en cuestión; y, de ser así, las formas, medios y canales para hacerlo.
- (ii) Distribución: El autor o titular del mismo es el único que puede autorizar o prohibir, que la obra, ya reproducida, sea puesta a disposición del público, mediante su venta, canje, permuta u otra forma de transmisión de la propiedad, alquiler, préstamo público o cualquier otra modalidad de uso o explotación.
- (iii) Traducción, adaptación, arreglo o transformación. Por estos derechos, el autor o titular de los mismos es el único que puede autorizar, o prohibir, la traducción, adaptación, arreglo u otra transformación de la obra”, p. 1.

⁵⁰ Véase la Resolución 701/2018 del Consejo de Transparencia y Buen Gobierno de España.

al código fuente de sistemas informáticos en virtud de esta protección proveniente de los derechos de autor. Ahora bien, ¿Sería posible que en el Perú una solicitud de esta naturaleza sea resuelta en términos similares?

Frente a esta interrogante, debemos recurrir a la Ley de Transparencia y Acceso a la Información Pública, aprobada por la Ley N° 27806, que en su artículo 3°⁵¹ consagra el denominado principio de máxima divulgación⁵² que deben de mantener las entidades públicas. La regla general es que toda información que posea el Estado es pública; sin embargo, existen excepciones a esta regla. Estas excepciones están desarrolladas en los artículos 15°⁵³ (información secreta), 15-A⁵⁴ (información reservada) y

⁵¹ Artículo 3.- Principio de publicidad

Todas las actividades y disposiciones de las entidades comprendidas en la presente Ley están sometidas al principio de publicidad. Los funcionarios responsables de brindar la información correspondiente al área de su competencia deberán prever una adecuada infraestructura, así como la organización, sistematización y publicación de la información a la que se refiere esta Ley.

⁵² Sobre el particular, el Tribunal Constitucional (2010) ha indicado lo siguiente en el Exp. No 05777-2008-PHC/TC:

“El “principio de máxima divulgación”, que tal como ha sido desarrollado por la Corte Interamericana de Derechos Humanos, “establece la presunción de que toda información es accesible, sujeta a un sistema restringido de excepciones”, (“Caso Claude Reyes y otros vs. Chile”), aun cuando dicha información no califique como pública, ésta deberá ser brindada a quien la solicite, siempre que justifique las razones por las cuáles su pedido deba ser atendido. y es que, tal como ha sido desarrollado en la STC N° 2579-2003-HD/TC, “la publicidad en la actuación de los poderes públicos constituye la regla general, y el secreto, cuando cuente con cobertura constitucional, la excepción” (...). (Considerando 15)

⁵³ Artículo 15.- Excepciones al ejercicio del derecho: Información Secreta

El derecho de acceso a la información pública no podrá ser ejercido respecto a la información expresamente clasificada como secreta, que se sustente en razones de seguridad nacional, en concordancia con el artículo 163 de la Constitución Política del Perú, que además tenga como base fundamental garantizar la seguridad de las personas y cuya revelación originaría riesgo para la integridad territorial y/o subsistencia del sistema democrático, así como respecto a las actividades de inteligencia y contrainteligencia del CNI dentro del marco que establece el Estado de Derecho en función de las situaciones expresamente contempladas en esta Ley.

⁵⁴ Artículo 15-A.- Excepciones al ejercicio del derecho: Información reservada

El derecho de acceso a la información pública no podrá ser ejercido respecto de la información clasificada como reservada. En consecuencia la excepción comprende únicamente los siguientes supuestos:

15-B⁵⁵ (información confidencial) de la misma norma. Así, los códigos fuentes de los *softwares* estarían protegidos por el secreto comercial⁵⁶ o también denominado secreto empresarial⁵⁷ (es decir, dentro de la cate-

1. La información que por razones de seguridad nacional en el ámbito del orden interno cuya revelación originaría un riesgo a la integridad territorial y/o la subsistencia del sistema democrático.

⁵⁵ “Artículo 15-B.- Excepciones al ejercicio del derecho: Información confidencial El derecho de acceso a la información pública no podrá ser ejercido respecto de lo siguiente:

1. La información que contenga consejos, recomendaciones u opiniones producidas como parte del proceso deliberativo y consultivo previo a la toma de una decisión de gobierno, salvo que dicha información sea pública. Una vez tomada la decisión, esta excepción cesa si la entidad de la Administración Pública opta por hacer referencia en forma expresa a esos consejos, recomendaciones u opiniones.

2. La información protegida por el secreto bancario, tributario, comercial, industrial, tecnológico y bursátil que están regulados, unos por el inciso 5 del artículo 2 de la Constitución, y los demás por la legislación pertinente. (...)”.

⁵⁶ La OMPI (2023) define al secreto comercial de la siguiente manera:

Los secretos comerciales son derechos de propiedad intelectual (PI) sobre información confidencial que pueden ser vendidos o concedidos en licencia. Por lo general, para considerarse secreto comercial, la información debe ser: (i) valiosa desde el punto de vista comercial puesto que es secreta; (ii) conocida únicamente por un número limitado de personas; y, (iii) objeto de medidas razonables para mantenerla en secreto por parte de la persona que legítimamente la controla, incluido el uso de acuerdos de confidencialidad entre asociados y empleados. La adquisición, utilización o divulgación no autorizada de esa información secreta de manera contraria a los usos comerciales honestos por otras personas se considera una práctica desleal y una violación de la protección del secreto comercial, p. 1.

⁵⁷ La Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales (2018) indicó lo siguiente sobre la distinción del secreto comercial, empresarial y tecnológico:

La legislación nacional, al igual que la doctrina y la legislación internacional, tienden a considerar al secreto comercial, secreto industrial y secreto tecnológico como parte de un todo, denominándolos en conjunto como secreto empresarial.

En ese sentido, el secreto empresarial es definido como aquel conocimiento no difundido susceptible de ser explotado económicamente, y que puede estar referido al proceso de producción de un bien (en cuyo caso estaremos ante un secreto industrial), al proceso de comercialización de un bien o servicio (en cuyo caso estaremos ante un secreto comercial), o a un nuevo conocimiento como resultado

goría de información confidencial), de acuerdo a lo previsto en el numeral 2 del artículo 15-B de la norma, ya que es una información que tiene un valor de mercado y que puede ser utilizada o comercializada por un tercero para obtener un beneficio económico. Adicionalmente, los códigos fuente de los *softwares* utilizados en el ámbito militar y de inteligencia podrían considerarse también incorporados dentro del rubro de información secreta al estar inmersos en el literal c) del artículo 15 (“Desarrollos técnicos y/o científicos propios de la defensa nacional”).

Por otro lado, debemos añadir que los códigos fuentes podrían también estar inmersos dentro de la categoría de secreto empresarial, para efectos de la aplicación de la Ley de Represión de la Competencia Desleal, aprobada por el Decreto Legislativo N° 1044. El artículo 13.a)⁵⁸ de dicha norma indica que constituye un acto de violación de secretos empresariales la acción de divulgar o explotar secretos empresariales ajenos a los que se haya tenido acceso legítimamente con deber de reserva o ilegítimamente sin autorización de su titular. En ese sentido, dicho acto de divulgación configuraría una infracción administrativa sujeta a las sanciones indicadas en el artículo 52⁵⁹ de la norma.

de un proceso de investigación científica o técnica (en cuyo caso se considera que existe un secreto tecnológico, al que se cataloga como un bien intangible, p. 3.

⁵⁸ Artículo 13.- Actos de violación de secretos empresariales.-

Consisten en la realización de actos que tengan como efecto, real o potencial, lo siguiente:

- a) Divulgar o explotar, sin autorización de su titular, secretos empresariales ajenos a los que se haya tenido acceso legítimamente con deber de reserva o ilegítimamente;
- b) Adquirir secretos empresariales ajenos por medio de espionaje, inducción al incumplimiento de deber de reserva o procedimiento análogo.

⁵⁹ Artículo 52.- Parámetros de la sanción.-

52.1.- La realización de actos de competencia desleal constituye una infracción a las disposiciones de la presente Ley y será sancionada por la Comisión bajo los siguientes parámetros:

52.2.- Los porcentajes sobre los ingresos brutos percibidos por el infractor, relativos a todas sus actividades económicas, correspondientes al ejercicio inmediato anterior al de la resolución de la Comisión indicados en el numeral precedente no serán considerados como parámetro para determinar el nivel de multa correspondiente en los casos en que el infractor: i) no haya acreditado el monto de ingresos brutos percibidos relativos a todas sus actividades económicas, correspondientes a dicho ejercicio; o, ii) se encuentre en situación de reincidencia.

La Secretaría de Gobierno y Transformación Digital de la Presidencia del Consejo de Ministros del Perú es el ente rector en materia de gobierno digital que comprende tecnologías digitales, identidad digital, interoperabilidad, servicio digital, datos, seguridad digital y arquitectura digital⁶⁰ y desarrolla guías sobre la materia. En su guía titulada “Lineamientos de servicios digitales” podemos hallar algunas recomendaciones sobre los *softwares* que deberían contratar las entidades públicas. En relación a la transparencia algorítmica, podemos rescatar lo indicado en la recomendación 15⁶¹ (“Datos abiertos por defecto”) y 16⁶² (“Desarrolla en código abierto”), que establecen que las entidades

52.3.- La reincidencia se considerará circunstancia agravante, por lo que la sanción aplicable no deberá ser menor que la sanción precedente.

52.4.- Para calcularse el monto de las multas a aplicarse de acuerdo a la presente Ley, se utilizará la UIT vigente a la fecha de pago efectivo.

52.5.- La multa aplicable será rebajada en un veinticinco por ciento (25%) cuando el infractor cancele el monto de la misma con anterioridad a la culminación del término para impugnar la resolución de la Comisión que puso fin a la instancia y en tanto no interponga recurso impugnativo alguno contra dicha resolución.

⁶⁰ El artículo 8 de la Ley de Gobierno Digital, aprobada por el Decreto Legislativo N° 1412, indica lo siguiente sobre las funciones de la Secretaría de Gobierno y Transformación Digital:

“Artículo 8.- Ente Rector en materia de Gobierno Digital

La Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, es el ente rector en materia de gobierno digital que comprende tecnologías digitales, identidad digital, interoperabilidad, servicio digital, datos, seguridad digital y arquitectura digital. Dicta las normas y establece los procedimientos en materia de gobierno digital y, es responsable de su operación y correcto funcionamiento”.

⁶¹ La Secretaría de Gobierno y Transformación Digital (2023a) indica lo siguiente:

“15. Datos abiertos por defecto:

Los datos deben ser abiertos y disponibles de manera inmediata, sin comprometer el derecho a la protección de los datos personales de los ciudadanos. Con esto, permitimos que otras entidades públicas, privadas, la sociedad civil y la academia, contribuyan fácilmente con la mejora de servicios y la toma de decisiones en los diferentes niveles del Gobierno” (p. 1).

⁶² La Secretaría de Gobierno y Transformación Digital (2023a) indica lo siguiente:

“16. Desarrolla en código abierto:

Haz uso de lenguajes de programación bajo licencias de uso libre que permitan a las comunidades y otras entidades reusar el código y proponer mejoras. Si existieran impedimentos de seguridad por los que no es posible abrir el código, puedes explicar las razones” (p. 1).

públicas deben de buscar *softwares* que sean de código abierto⁶³, es decir, de uso y acceso libre y que puedan ser reutilizados por otras entidades públicas. Sin perjuicio de lo anterior, debemos de advertir que estos *softwares* de código abierto no implican necesariamente que se habilite a las Administraciones Públicas a compartir sus códigos fuente.

Sin perjuicio de lo anterior, debemos indicar que el artículo 29⁶⁴ de la Ley del Gobierno Digital prevé un régimen especial para *softwares* adquiridos por la Administración Pública que podrían estar sujetos a un régimen de transparencia algorítmica que habilitaría a las entidades a poder compartir su código fuente frente a una solicitud de acceso a la información pública. Nos referimos al Software Público Peruano.

El Software Público Peruano es un régimen aplicable a *softwares* que habilitan que las entidades que los adquirieron puedan compartir sus códigos fuente con otras entidades a través del denominado Portal del Software Público Peruano⁶⁵, con la finalidad que sean reutilizados y

⁶³ La Secretaría de Gobierno y Transformación Digital (2023b) indica los siguientes beneficios del uso de códigos abiertos en su “Guía de uso de tecnologías para servicios digitales”:

- (i) Resolver problemas comunes con tecnologías de código abierto actualmente disponibles y funcionando.
- (ii) Ahorrar tiempo y recursos evitando el desarrollo de soluciones muy particulares o para problemas poco frecuentes.
- (iii) Exigir menores tiempos de implementación y costos de ejecución.
- (iv) Interoperar con soluciones de código cerrado mediante software abierto” (p. 1).

⁶⁴ Artículo 29.- Reutilización de Software

Las entidades de la Administración Pública titulares de Software Público Peruano, desarrollado mediante la contratación de terceros o por personal de la entidad para soportar sus procesos o servicios, adoptan las medidas necesarias a fin de obtener la titularidad exclusiva sobre los derechos patrimoniales del referido Software Público Peruano.

Todas las entidades de la Administración Pública deben compartir Software Público Peruano bajo licencias libres o abiertas que permitan (i) usarlo o ejecutarlo, (ii) copiarlo o reproducirlo, (iii) acceder al código fuente, código objeto, documentación técnica y manuales de uso, (iv) modificarlo o transformarlo en forma colaborativa, y (v) distribuirlo, en beneficio del Estado Peruano.

⁶⁵ El artículo 1 del Decreto Supremo que crea el Portal de software Público Peruano y establece disposiciones adicionales sobre el software Público Peruano, aprobado por el Decreto Supremo N° 051-2018-PCM, indica lo siguiente:

“Artículo 1.- Creación del Portal de Software Público Peruano

mejorar la calidad de los servicios públicos. Dentro de las condiciones⁶⁶ que deben de cumplir estos *softwares*, encontramos a las siguientes: (i) deben estar bajo licencias libres o abiertas que permitan ser usados, copiados, modificados y distribuidos⁶⁷; (ii) soportan procesos o

Créase el Portal de Software Público Peruano (PSPP), como plataforma oficial que facilita el acceso a Software Público Peruano, que las entidades de la Administración Pública están en condiciones de compartir bajo licencias libres o abiertas que permitan (i) usarlo o ejecutarlo, (ii) copiarlo o reproducirlo, (iii) acceder al código fuente, código objeto, documentación técnica y manuales de uso, (iv) modificarlo o transformarlo en forma colaborativa, y (v) distribuirlo, en beneficio del Estado Peruano.

El Portal de Software Público Peruano - PSPP es administrado por la Secretaría de Gobierno Digital (SEGDI) de la Presidencia del Consejo de Ministros, accediendo a través del dominio www.softwarepublico.gob.pe".

⁶⁶ El artículo 8 de la Directiva N° 001-2019-PCM-SEGDI, "Directiva para compartir y usar Software Público Peruano", indica lo siguiente:

"Artículo 8°.- Características del Software Público Peruano

8.1 Es de titularidad de la entidad de la Administración Pública, exceptuando y respetando los componentes del software propietario o licenciado y los principios del software libre, según sea el caso.

8.2 Soporta procesos o funcionalidades que tengan o puedan tener alcances, objetivos, características o actividades similares en las entidades de la Administración Pública.

8.3 El código fuente y código objeto derivado es liberado y puesto a disposición mediante una licencia libre o abierta.

8.4 Tener como mínimo la documentación siguiente: 1. Diccionario de Datos, 2. Manual de usuario o equivalente, 3. Documentación técnica de desarrollo (deseable incluir el Manual de Operaciones o documento equivalente) y 4. Manual de instalación y configuración, los mismos que deben estar publicados bajo una licencia libre o abierta. Dicha documentación debe ser la última versión actualizada y vigente. Opcionalmente, podrá brindar la siguiente documentación: análisis funcional, diseño y estructura del software, arquitectura y componentes, conjunto de pruebas funcionales y no funcionales, casos de uso del proceso de negocio y sistema. La documentación a compartir debe encontrarse en texto simple, se sugiere usar formatos de tipo: formato de documento portátil (PDF por sus siglas en inglés), formato de documento abierto (ODF por sus siglas en inglés), entre otros".

⁶⁷ El artículo 4 del Decreto Supremo que crea el Portal de software Público Peruano y establece disposiciones adicionales sobre el software Público Peruano, aprobado por el Decreto Supremo N° 051-2018-PCM, indica lo siguiente:

"Artículo 4.- Del Software Público Peruano

El Software Público Peruano es aquel software o programa de ordenador de titularidad de una entidad de la Administración Pública, cuyo desarrollo es contratado o efectuado directamente por el personal de dicha entidad para soportar

funcionalidades que tengan o puedan tener alcances, objetivos, características o actividades similares en las entidades de la Administración Pública; (iii) el código fuente y código objeto derivado es liberado y puesto a disposición mediante una licencia libre o abierta; y, (iv) tienen como mínimo la siguiente documentación: diccionario de datos, manual de usuario o equivalente, documentación técnica de desarrollo y manual de instalación y configuración, los mismos que deben estar publicados bajo una licencia libre o abierta.

Ahora bien, debemos de indicar que en el Perú se han dado algunas aproximaciones a la problemática de la transparencia algorítmica. En primer lugar, en la legislación se ha incorporado un mecanismo que, si bien no fue diseñado para ser una herramienta de transparencia algorítmica, lo cierto es que en la práctica sí lo constituye. Nos referimos al denominado “informe técnico previo de evaluación de software”. En el año 2005, la Ley que norma el uso, adquisición y adecuación del software en la administración pública, aprobada por la Ley N° 28612, estableció que si una entidad pública deseaba adquirir un *software* debía realizar un informe técnico previo de evaluación de software a cargo de su oficina de informática, con la finalidad de analizar las condiciones de uso, mantenimiento, seguridad y otras de estos sistemas⁶⁸. Además, este

sus procesos o servicios, es financiado con fondos públicos, y puede ser puesto a disposición para ser usado, copiado, modificado y distribuido bajo una licencia libre o abierta”.

⁶⁸ El artículo 5 de la Ley que norma el uso, adquisición y adecuación del software en la administración pública, aprobada por la Ley N° 28612, indica lo siguiente:

“Artículo 5.- Estudio, evaluación e informe previo

El uso o adquisición de licencias de software en la administración pública requiere del Informe Previo de Evaluación de la Oficina de Informática, que determine el tipo de licencia de software que resulte más conveniente para atender el requerimiento formulado. El Informe deberá contener, bajo responsabilidad, un análisis comparativo de valores de mercado, así como de los costos y beneficios en el corto, mediano y largo plazo de las licencias existentes. En el caso de existir un sólo tipo de software, el Informe se limitará a certificar este hecho. El Informe se hará de conocimiento público en la página web de la entidad que corresponda, salvo los casos de reserva por seguridad nacional, conforme lo disponga el reglamento.

La entidad procurará que la adquisición responda a los principios de vigencia y neutralidad tecnológica, transparencia, eficiencia y a los criterios de austeridad y ahorro de los recursos públicos”.

informe debe ser publicado⁶⁹ en el portal institucional de cada entidad.

Los requisitos mínimos del informe técnico previo de evaluación de *software* son los siguientes, de acuerdo a lo previsto en el Anexo del Reglamento de la Ley N° 28612 - Ley que norma el uso, adquisición y adecuación del software en la administración pública, aprobado por el Decreto Supremo N° 024-2006-PCM:

- Nombre del área.
- Responsables de la evaluación.
- Cargos.
- Fecha.
- Justificación (descripción de la necesidad que se pretende satisfacer y que deriva de los requerimientos formulados por las áreas usuarias).
- Alternativas (se incluyen los productos software alternativo a ser comparados, sin incluir proveedores).
- Análisis comparativo técnico.
- Análisis comparativo de costo - beneficio. Se analizan los siguientes: (i) el licenciamiento; (ii) el *hardware* necesario para su funcionamiento; (iii) el soporte y mantenimiento externo; (iv) personal y mantenimiento interno; (v) capacitación; (vi) costos operativos de TI; (vii) impacto en el cambio de plataforma; (viii) tiempo de recuperación (*Downtime*) y tiempo en el que se va a entregar la solución con las condiciones exigidas por la empresa (*Time to market*); y, (ix) garantías comerciales aplicables.

⁶⁹ El artículo 8 del Reglamento de la Ley N° 28612 - Ley que norma el uso, adquisición y adecuación del software en la administración pública, aprobado por el Decreto Supremo N° 024-2006-PCM, indica lo siguiente:

“Artículo 8.- Publicación del Informe Técnico Previo de Evaluación de Software.

El informe será publicado en la sección de transparencia de la página web institucional, antes de convocarse al proceso de selección correspondiente, bajo responsabilidad del funcionario competente. Si la institución no tuviera página web institucional, será publicado en el Portal del Sistema Electrónico de Adquisiciones y Contrataciones del Estado (SEACE) del Consejo Superior de Contrataciones y Adquisiciones del Estado (CONSUCODE), al momento de ser convocado y como parte de las Bases del proceso, para lo cual deberá remitirle al CONSUCODE la información en archivos electrónicos”.

- Conclusiones.
- Firmas.

Como podemos apreciar, existen aspectos valiosos del informe sobre las condiciones de uso de los *softwares*, tales como el *hardware* necesario, las condiciones de mantenimiento necesarias, la capacitación de los equipos técnicos a cargo del mantenimiento, los costos operativos, entre otros. A pesar de que hemos indicado que en la práctica el informe constituye una herramienta de transparencia algorítmica, lo cierto es que este fue diseñado como un mecanismo de análisis de la idoneidad del sistema informático, de cara al futuro procedimiento de contratación pública para la adquisición del *software*.

En segundo lugar, la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Ministerio de Justicia (en adelante, la “Dirección”) ha tratado la problemática de la publicidad del código fuente de *softwares* utilizados en los procesos electorales por una solicitud de acceso a la información pública (lo que implica un determinado escenario de transparencia algorítmica), con motivo de una consulta formulada por la Oficina Nacional de Procesos Electorales (ONPE). En dicha consulta, la ONPE preguntó si una relación de documentos denominados “Activos de Información”⁷⁰ (que incluía códigos fuentes y documentos técnicos sobre sistemas informáticos utilizados en los procesos electorales y su infraestructura) podían ser clasificados dentro de alguna excepción al acceso a la información

⁷⁰ La Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales (2018) indicó que, dentro de la categoría de Activos Informáticos, la ONPE había incluido a los siguientes:

- Los productos software y sus códigos fuente.
- Los documentos técnicos que describen de forma detallada la arquitectura de los sistemas informáticos y aplicaciones que por sus características, uso y tratamiento de información protegida por ley requiere su protección para evitar riesgos de vulnerabilidad técnica.
- Los documentos con la información detallada de los nombres de los servidores, aplicaciones de bases de datos, almacenamiento y conexiones de bases de datos.
- Los documentos técnicos que describen de forma detallada la arquitectura de la infraestructura de la Tecnología de la Información. (p. 2)

pública. Sobre el particular, la Dirección indicó⁷¹ que la Ley de Transparencia y Acceso a la Información Pública no trata la seguridad de la información en los procesos electorales. Sin embargo, por el mandato constitucional de la ONPE (vinculado a la realización de los procesos electorales), la entidad podría estar habilitada a limitar el acceso a dicha información “toda vez que de ser develada podría poner en riesgo cierto y concreto la seguridad del proceso electoral, más allá del régimen de excepciones de la Ley de Transparencia y Acceso a la Información Pública” (Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales, 2018)⁷².

⁷¹ La Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales (2018) indicó lo siguiente:

Corresponde a la ONPE la organización y ejecución del proceso electoral, lo que supone el diseño e implementación de una serie de medidas, acciones y procedimientos dirigidos a su realización, estableciéndose metas y objetivos; en tanto que, la ejecución, comporta la materialización y puesta en marcha de dichas acciones y procedimientos, y que se desarrollan a lo largo de las distintas etapas del proceso electoral. En tal sentido, los entes electorales deben perseguir que las elecciones sean transparentes, excluyendo cualquier posibilidad de fraude electoral; por lo que, no habiéndose contemplado en la Ley 27806 algún supuesto que garantice la seguridad de la información referida a los procesos electorales, se debería evaluar si la entrega de la información generaría un riesgo real y cierto a la seguridad del resultado del proceso electoral, haciendo inviable el cumplimiento de la finalidad constitucional asignada a los entes electorales en la democracia peruana. (...) Estos parámetros ofrecen a la ONPE, a juicio de esta Autoridad Nacional, un argumento de orden constitucional para limitar el acceso a la información pública de toda aquella información que, de ser develada, podría poner en riesgo cierto y concreto la seguridad del proceso electoral y, con ella, la finalidad misma del sistema electoral, más allá del régimen de excepciones que establece la Ley de Transparencia y Acceso a la Información Pública. (pp. 4 - 5)

⁷² Dirección General de Transparencia, A. a. (2018). Opinión Consultiva N° 31-2018-JUS/DGTAIPD. Lima: Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales. Obtenido de <https://www.gob.pe/institucion/antaip/informes-publicaciones/1368448-oc-n-31-2018-jus-dgtaipd-si-la-relacion-de-activos-de-informacion-que-se-encuentra-en-posesion-o-control-de-la-gerencia-de-informatica-y-tecnologia-electoral-de-la-oficina-nacional-de-pr>

Cabe destacar que la tendencia actual⁷³ en mecanismos de transparencia algorítmica son los modelos de reportes periódicos, como el implementado recientemente por Reino Unido⁷⁴. En dicho país, el Central Digital and Data Office y el Centre for Data Ethics and Innovation⁷⁵, han desarrollado un proyecto denominado *Algorithmic*

⁷³ Britain Thinks (2021) ha destacado los ejemplos los reportes de transparencia algorítmica de las ciudades de Nueva York y Helsinki (p. 43). Sobre ambos ejemplos, Britain Thinks (2021) realizó un estudio e identificó lo siguiente:

Overall, the Helsinki model has high appeal amongst all participants. They are positive about the information being in a centralised register and assume that people would be able to locate this information easily. In addition, they appreciate the simple headlines and summaries that are provided on the home page, and value the option of being able to click on 'read more' if they require more detailed information. (...) On initial exposure to the New York model, participants raise concerns about the length of the content and feel that it is not as user friendly as the first example. Participants like the clear headings, but without the filter for additional information (as in the Helsinki model), participants either feel this is the right level of information or too much. (...) Most participants assume that this level of information is not targeted to the public, and is more likely to be suitable to academics or experts. In addition, a few participants raise concerns about the accessibility of the information because of its format and thought that some people would not be able to access it. There was some confusion about whether this would need to be downloaded from a website or whether it would open in a web browser. (pp. 43 - 44)

Britain Thinks. (2021). *Complete transparency, complete simplicity: How can the public sector be meaningfully transparent about algorithmic decision making?* London: Britain Thinks. Obtenido de https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/995014/Complete_transparency_complete_simplicity_-_Accessible.pdf

⁷⁴ Véase: <https://www.gov.uk/government/collections/algorithmic-transparency-recording-standard-hub>

⁷⁵ El Central Digital and Data Office y el Centre for Data Ethics and Innovation (2023), indican lo siguiente sobre su proyecto:

The Algorithmic Transparency Recording Standard helps public sector organisations provide clear information about the algorithmic tools they use, and why they're using them.

Algorithmic transparency means being open about how algorithmic tools support decisions. This includes providing information on algorithmic tools and algorithm-assisted decisions in a complete, open, understandable, easily-accessible, and free format. (...) The Algorithmic Transparency Recording Standard is part of the government's National Data Strategy. The strategy has a commitment to explore an appropriate and effective way to deliver greater transparency on algorithm-

Transparency Recording Standard, compuesto por reportes periódicos sobre las condiciones de uso, mantenimiento y de vulnerabilidades de lo que denominan “herramienta algorítmica”⁷⁶.

El Central Digital and Data Office y el Centre for Data Ethics and Innovation and Innovation (2023)⁷⁷, han estructurado el reporte en dos (2) secciones: (i) el Tier 1⁷⁸ (“donde se incluye una breve descripción no técnica de la herramienta algorítmica, una visión general de la

assisted decision making in the public sector. The National AI Strategy reiterated this commitment, with an action to conduct research that will help develop a cross-government standard for algorithmic transparency. (p. 1)

⁷⁶ El Central Digital and Data Office y el Centre for Data Ethics and Innovation and Innovation (2023) han señalado lo siguiente sobre las herramientas algorítmicas y el programa denominado *Algorithmic Transparency Recording Standard*:

An algorithmic tool is a product, application, or device that supports or solves a specific problem, using complex algorithms. You can develop a tool in-house or buy from a third party. To help non-experts understand this work, we’re using ‘algorithmic tool’ as a deliberately broad term that covers different applications of AI and complex algorithms. (...) The Algorithmic Transparency Recording Standard is most relevant for algorithmic tools that either: (i) have a significant influence on a decision-making process with direct or indirect public effect, or (ii) directly interact with the general public, p. 1.

⁷⁷ Central Digital and Data Office y Centre for Data Ethics and Innovation. (5 de Enero de 2023). Algorithmic Transparency Recording Standard Hub. Obtenido de GOV. UK: <https://www.gov.uk/government/collections/algorithmic-transparency-recording-standard-hub>

⁷⁸ El Central Digital and Data Office y el Centre for Data Ethics and Innovation and Innovation (2023), incorpora la siguiente información en el Tier 1

Tier 1 information

How and why you’re using the algorithmic tool (1.2)

Explain:

- how your tool works
- how your tool is incorporated into your decision making process
- what problem you’re aiming to solve using the tool, and how it’s solving the problem
- your justification or rationale for using the tool
- How people can find out more information (1.3 and 1.4)

Explain how people can find out more about the tool or ask a question - including offline options and a contact email address of the responsible organisation, team or contact person (p. 1)

herramienta y por qué se utiliza”)⁷⁹; y, (ii) el Tier 2⁸⁰ (“donde se incluye información técnica más detallada, como detalles específicos sobre el funcionamiento de la herramienta y los datos que utiliza”).

Frente a lo anterior, podemos identificar que existen tres (3) escenarios de transparencia algorítmica que debería considerar la Administración Pública:

Escenario 1: El contenido del código fuente debe ser de acceso público y sin restricciones en aplicación del principio de transparencia y el derecho a la defensa.

El código fuente es fundamental para cualquier sistema informático y el administrado tiene el derecho a conocer la totalidad de su contenido (en aplicación del principio de transparencia), debido a que de lo contrario se puede generar una situación de indefensión, afectando el derecho a la defensa.

Este escenario ha sido recogida por el Consejo de Transparencia y Buen Gobierno de España en la Resolución 058/2021. En dicho caso, se trató una solicitud de acceso a la información pública de los siguientes aspectos del *software* utilizado en las pensiones: (i) el “algoritmo” del programa de cálculo de pensiones; (ii) ¿Cómo se realiza la conversión de días a años?; y, (iii) ¿Cómo los trata cuando hay días de cotización superpuestos?

El Consejo de Transparencia y Buen Gobierno (2021)⁸¹ declaró fundado el recurso y ordenó otorgar la información solicitada en un plazo

⁷⁹ Traducción propia.

⁸⁰ El Central Digital and Data Office y el Centre for Data Ethics and Innovation and Innovation (2023), incorpora la siguiente información en el Tier 2:

Tier 2 information

Section 1: Who owns and has responsibility for the algorithmic tool

(...)

Section 2: How the tool works in detail and what the rationale for its use is

(...)

Section 3: How the tool is integrated into the wider decision making process

(...)

Section 4: Technical specification and data

(...)

Section 5: Risks, mitigations and impact assessments (p. 1)

⁸¹ Consejo de Transparencia y Buen Gobierno. (2021). Resolución 058/2021. Madrid: Consejo de Transparencia y Buen Gobierno.

de diez (10) días hábiles, señalando que⁸²: “mientras que no se implementen mecanismos de rendición de cuentas y fiscalización de los poderes públicos sobre la transparencia de los algoritmos con garantías equivalentes (p.ej. auditorías independientes u órganos de supervisión), el único recurso para tales efectos es el acceso al algoritmo” (pp. 7 - 8).

Por otro lado, los sistemas informáticos pueden tener sesgos⁸³ debido a que funcionan en base a premisas establecidas por una persona o

⁸² El Consejo de Transparencia y Buen Gobierno (2021) indicó lo siguiente:

En el contexto actual de progresivo desarrollo e implantación la administración electrónica y uso creciente de la inteligencia artificial, los algoritmos están adquiriendo una relevancia decisiva, a la vez que se incrementa su complejidad. Pueden sustentar la toma de decisiones públicas o, directamente, ser fuente de decisiones automatizadas con consecuencias muy relevantes para las personas. Esta evolución está generando una creciente demanda ciudadana de transparencia de los algoritmos utilizados por las Administraciones públicas como condición inexcusable para preservar la rendición de cuentas y la fiscalización de las decisiones de los poderes públicos y, en último término, como garantía efectiva frente a la arbitrariedad o los sesgos discriminatorios en la toma de decisiones total o parcialmente automatizadas. Mientras no se instauran otros mecanismos que permitan alcanzar los fines señalados con garantías equivalentes –como podrían ser, por ejemplo, auditorías independientes u órganos de supervisión–, el único recurso eficaz a tales efectos es el acceso al algoritmo propiamente dicho, a su código, para su fiscalización tanto por quienes se puedan sentir perjudicados por sus resultados como por la ciudadanía en general en aras de la observancia de principios éticos y de justicia. (pp. 7 - 8)

⁸³ El Grupo Independiente de Expertos de Alto Nivel sobre Inteligencia Artificial (2018), ha indicado lo siguiente de los sesgos en la IA:

Los conjuntos de datos que utilizan los sistemas de IA (tanto con fines de formación como para su funcionamiento) pueden presentar sesgos históricos inadvertidos, lagunas o modelos de gestión incorrectos. El mantenimiento de dichos sesgos podría dar lugar a prejuicios y discriminación (in)directos e involuntarios contra determinados grupos o personas, lo que podría agravar los estereotipos y la marginación. La explotación intencionada de los sesgos (de los consumidores) o la competencia desleal también pueden provocar situaciones perjudiciales, como la homogeneización de los precios mediante la colusión o la falta de transparencia del mercado. Siempre que sea posible, los sesgos identificables y discriminatorios deberían eliminarse en la fase de recopilación de la información. Los propios métodos de desarrollo de los sistemas de IA (por ejemplo, la programación de algoritmos) también pueden presentar sesgos injustos. Esto se puede combatir mediante procesos de supervisión que permitan analizar y abordar el propósito, las restricciones, los requisitos y las decisiones del sistema de un modo claro y transparente. Además, la contratación de personas procedentes de diversos

entidad en su código fuente. También, éstos contienen errores (*bugs*) y son vulnerables a ataques informáticos. En esa línea, ningún sistema informático es infalible por lo que el administrado debería conocer dichas situaciones, a fin de ejercer su derecho a la defensa de maneja eficaz en el supuesto que exista alguna falla o vulneración del sistema.

Escenario 2: El contenido del código fuente no puede ser público, debido a que está protegido por los derechos de propiedad intelectual.

A pesar del anterior escenario, lo cierto es que estos programas informáticos son desarrollados por personas o empresas especializadas en el rubro de la programación, y que sus productos están protegidos por derechos morales y derechos patrimoniales, que fueran explicados anteriormente.

Este escenario ha sido considerado en su momento por el Consejo de Transparencia y Buen Gobierno de España en la Resolución 701/2018. En dicho caso, se trató una solicitud de acceso a la información pública de la siguiente información sobre la aplicación (el denominado sistema BOSCO) que permite al comercializador de energía eléctrica comprobar los requisitos para identificar a un consumidor vulnerable y otorgar un bono social (es decir, un descuento): (i) sus especificaciones técnicas; (ii) las pruebas para comprobar que cumplía con la especificación funcional; (iii) su código fuente; y, (iv) cualquier otro entregable que permita conocer el funcionamiento de la aplicación.

El caso se resolvió fundado en parte y se otorgó acceso a los siguientes: (i) las especificaciones técnicas; (ii) los resultados de las pruebas para comprobar que cumplía con la especificación funcional; y, (iii) cualquier otro entregable que permita conocer el funcionamiento de la aplicación. Por otro lado, se denegó la solicitud en el extremo al acceso al código fuente, debido al límite al derecho al acceso a la información previsto en el literal j del artículo 14.1⁸⁴ (secreto profesional y la propiedad

contextos, culturas y disciplinas puede garantizar la diversidad de opiniones y debería fomentarse. (p. 23)

⁸⁴ Artículo 14. Límites al derecho de acceso.

1. El derecho de acceso podrá ser limitado cuando acceder a la información suponga un perjuicio para:

(...)

j) El secreto profesional y la propiedad intelectual e industrial.

intelectual e industrial) de la Ley 19/2013, de 9 de diciembre, Ley de transparencia, acceso a la información pública y buen gobierno (en adelante, la “LTAIBG”). Teniendo en cuenta lo anterior, el Consejo de Transparencia y Buen Gobierno (2018)⁸⁵, indicó lo siguiente:

“Este límite se relaciona con la propia naturaleza de lo solicitado: el código fuente que sirve de soporte a la aplicación telemática que permite al comercializador de referencia comprobar que el solicitante del bono social cumple los requisitos para ser considerado consumidor vulnerable. (...) Puesto que el código fuente se expresa de forma escrita, resulta lógico pensar que el software puede ser protegido por el derecho de autor como obra literaria. Este es, en efecto, el enfoque vigente respecto de la protección del software en diversos tratados internacionales.”

Teniendo en cuenta a lo anterior, que el Estado ordene compartir todo el contenido del código fuente puede: (i) generar un daño a los derechos morales y patrimoniales (y que estaría sujeto a una indemnización); y, (ii) desincentivar la participación de estos particulares en las licitaciones de estos servicios. Sin perjuicio de lo anterior, el ciudadano promedio no suele contar con los conocimientos que le permitan entender los componentes y funciones de un código fuente. Así, se podrían implementar otros mecanismos para explicar su funcionamiento, como hacer que estén habilitados manuales de uso (con la explicación de detalles clave de los sistemas informáticos, como las premisas del sistema y sus posibles errores) y reportes periódicos de transparencia algorítmica (como el proyecto realizado en Reino Unido).

Escenario 3: Todo el contenido del código fuente no puede ser público debido a la protección de los derechos de propiedad intelectual involucrados (secreto comercial). Sin embargo, ello no elimina la posibilidad que la Administración asegure un nivel óptimo de transparencia algorítmica mediante otros mecanismos complementarios para explicar el funcionamiento del *software* al administrado, tales como reportes periódicos de transparencia algorítmica.

En este escenario, la Administración Pública realiza reportes periódicos de transparencia algorítmica sobre las condiciones de uso, mantenimiento y vulnerabilidades de los *softwares* que utiliza, asegurando también

⁸⁵ Consejo de Transparencia y Buen Gobierno . (2018). Resolución 701/2018. Madrid: Consejo de Transparencia y Buen Gobierno, p. 9.

la explicabilidad⁸⁶ del *software*. Además, dichos reportes aseguran un seguimiento de las condiciones de mantenimiento y el control de los riesgos de las vulnerabilidades de dichos *softwares*.

De igual modo, se debe de asegurar el acceso a documentos técnicos que cumplan con la finalidad explicar al ciudadano con un lenguaje claro, sencillo y accesible los términos y condiciones del funcionamiento de los *softwares*, tales como manuales de uso y especificaciones técnicas. Esto en línea con una adecuada Administración Digital, en la que la Administración Pública no solo debe poner al alcance información sino conocimiento, es decir, información procesada y accesible al ciudadano desarrollada con la finalidad de acercar los servicios públicos a los administrados.

Por otro lado, es importante resguardar que las oportunidades de colaboración entre el sector público y el privado no se vean desincentivadas. La publicación total del código fuente generaría que sus competidores o cualquier particular pueda copiar el código fuente del programa y utilizarlo para otra actividad con un fin lucrativo, pudiendo perjudicar los intereses económicos de la empresa o persona que haya desarrollado el código fuente. Sin perjuicio de lo anterior, en el supuesto que una Administración Pública adquiera un *software* con

⁸⁶ El Grupo Independiente de Expertos de Alto Nivel sobre Inteligencia Artificial (2018), ha indicado lo siguiente sobre la explicabilidad:

La explicabilidad es crucial para conseguir que los usuarios confíen en los sistemas de IA y para mantener dicha confianza. Esto significa que los procesos han de ser transparentes, que es preciso comunicar abiertamente las capacidades y la finalidad de los sistemas de IA y que las decisiones deben poder explicarse —en la medida de lo posible— a las partes que se vean afectadas por ellas de manera directa o indirecta. Sin esta información, no es posible impugnar adecuadamente una decisión. No siempre resulta posible explicar por qué un modelo ha generado un resultado o una decisión particular (ni qué combinación de factores contribuyeron a ello). Esos casos, que se denominan algoritmos de «caja negra», requieren especial atención. En tales circunstancias, puede ser necesario adoptar otras medidas relacionadas con la explicabilidad (por ejemplo, la trazabilidad, la auditabilidad y la comunicación transparente sobre las prestaciones del sistema), siempre y cuando el sistema en su conjunto respete los derechos fundamentales. El grado de necesidad de explicabilidad depende en gran medida del contexto y la gravedad de las consecuencias derivadas de un resultado erróneo o inadecuado, p. 16.

una licencia de código abierto, se podría analizar la conveniencia de un mecanismo de transparencia que incluya componentes claves y/o la totalidad del código fuente; y, con ello: (i) otorgar un nivel reforzado de transparencia algorítmica (es decir, dar a conocer al administrado todo el contenido del funcionamiento de las condiciones de uso, mantenimiento y vulnerabilidades de los *softwares*); (ii) permitir que dicho nivel de publicidad coexista con un sistema de reportes periódicos (y sus beneficios, como el seguimiento de las condiciones de mantenimiento y gestión de los riesgos de las vulnerabilidades del *software*); y, (iii) generar espacios para que los *softwares* sean utilizados en iniciativas como el Software Público Peruano y que sean compartidos con otras entidades.

V. Conclusiones

- Las Administraciones Públicas en el Perú ya han implementado actuaciones automatizadas y procedimientos administrativos automatizados, en el marco del denominado derecho de los administrados a relacionarse electrónicamente con la Administración. Este derecho no solo habilita al administrado de tomar la libre decisión de relacionarse con la Administración usando medios electrónicos, sino también de decidir la interrupción de estos medios y retornar a la tramitación propia de un procedimiento ordinario.
- La transparencia algorítmica es el nivel de publicidad activa o pasiva sobre las condiciones de uso, mantenimiento y vulnerabilidades de los *softwares* que sean utilizados en alguna actuación automatizada o procedimiento administrativo automatizado. La Administración Pública debe mantener niveles óptimos de transparencia algorítmica sobre sus actuaciones administrativas automatizadas y procedimientos administrativos automatizados, con la finalidad de asegurar el principio de transparencia y derechos fundamentales vinculados a entornos digitales, tales como: (i) el derecho a la información; y, (ii) el derecho a la defensa de los administrados. En esa línea, las entidades públicas deben incorporar mecanismos activos y pasivos de transparencia algorítmica, tales como: (i) la publicación de reportes periódicos, manuales de uso y documentos con especificaciones técnicas; y, (ii) la atención de solicitudes de información.
- La publicidad total del contenido del código fuente es un elemento de un determinado nivel de transparencia algorítmica y no una

condición inherente para un nivel óptimo de transparencia algorítmica. Un nivel óptimo de transparencia algorítmica incluye las condiciones de mantenimiento y vulnerabilidades del *software*, lo que solo se podría identificar en el transcurso del tiempo del uso del mismo, mediante mecanismos de reportes periódicos (es decir, mecanismos que aseguren el seguimiento en el tiempo del sistema) que detallen cómo la Administración Pública ejecuta las condiciones de mantenimiento y control de los riesgos de las vulnerabilidades de los mismos.

- La publicidad de un *software* sin una licencia de código abierto podría: (i) configurar una de las excepciones al derecho de acceso a la información pública, de acuerdo a lo previsto en la Ley de Transparencia y Acceso a la Información Pública (secreto comercial - información confidencial); (ii) configurar una vulneración al secreto comercial o empresarial, lo que a su vez constituye una infracción administrativa y un posible daño indemnizable cuyo resarcimiento pueda ser solicitado en la vía civil; y, (iii) desincentivar que las empresas y profesionales especializados en el diseño y elaboración de *software* participen en las licitaciones para la elaboración y ejecución de estos programas en la Administración Pública. Además, teniendo en cuenta lo anterior, el nivel de transparencia sobre el código fuente deberá estar acorde a lo pactado entre el desarrollador (quien es titular del derecho moral sobre el *software*) y la Administración Pública, debiendo respetarse los términos y condiciones pactados sobre su uso y divulgación.

El uso del big data en los procesos electorales. El sufragio ¿Representa la verdadera voluntad popular? Una mirada desde el sistema jurídico argentino

Lucrecia Contardi Gonzáles*

Resumen.- El uso de Big Data ha transformado los procesos electorales, influyendo en la toma de decisiones, la segmentación de votantes y la optimización de campañas. Este estudio analiza cómo las plataformas digitales y redes sociales impactan en la difusión de información electoral y examina los desafíos éticos y de privacidad asociados al uso de datos personales en contextos de participación ciudadana y sufragio.

Palabras clave.- Big Data – Procesos Electorales – Sufragio – Participación ciudadana – Ética.

Abstract.- The use of Big Data has transformed electoral processes, influencing decision-making, voter segmentation, and campaign optimization. This study analyzes how digital platforms and social media impact the dissemination of electoral information and examines the ethical and privacy challenges associated with the use of personal data in the context of citizen participation and voting.

Keywords.- Big Data – Electoral processes – Suffrage – Citizen Participation- Ethics.

* Abogada y Escribana- Facultad de Ciencias Jurídicas y Sociales-Universidad Nacional de La Plata. Especialista en Derecho Informático- Universidad de Buenos Aires. Auxiliar docente con funciones de adjunta en Introducción al Estudio de las Ciencias Sociales actualmente; Auxiliar alumna y docente con funciones de adjunta interina en Historia Constitucional -2013-2023-. Profesora en la orientación de Derecho Informático y Protección de Datos Personales- FCJyS – UNLP -2023-.

I. Introducción

En la actualidad, los procesos democráticos enfrentan transformaciones profundas a partir de la irrupción de las tecnologías digitales en todos los aspectos de la vida social. El modo en que las personas se informan, se comunican y participan políticamente ha cambiado radicalmente en las últimas dos décadas. En este contexto, la relación entre tecnología, datos personales y participación ciudadana plantea interrogantes centrales sobre el funcionamiento de la democracia contemporánea.

Dentro de ese entramado, el sufragio –derecho-deber por excelencia– no ha permanecido ajeno a estos cambios. De igual modo, los partidos políticos, actores fundamentales en la canalización de la voluntad popular, han debido adaptarse a un nuevo ecosistema comunicacional y tecnológico que redefine las estrategias electorales, la forma de interpelar al electorado y la construcción del vínculo entre representantes y representados. La incorporación de herramientas digitales ha modificado las dinámicas de las campañas, los métodos de persuasión y, especialmente, la forma en que se interpreta y se busca influir en el comportamiento del votante.

Hoy nos encontramos inmersos en una sociedad completamente digital, atravesada por la denominada Industria 4.0 o Cuarta Revolución Industrial, caracterizada por la integración de tecnologías como la inteligencia artificial, el internet de las cosas, el análisis masivo de datos (Big Data) y la automatización. Este proceso de transformación ha sido acelerado por diversos factores, entre ellos, la emergencia sanitaria provocada por el Covid-19, que intensificó el uso de internet y multiplicó el acceso desde diversos dispositivos, en especial los teléfonos móviles.

Si bien aún la concepción del acceso a Internet como un derecho humano fundamental plasmado en la Constitución Nacional argentina dista mucho de ser una realidad, no menos cierto es que vivimos en una sociedad híper-conectada, y que la red de redes es un recurso esencial por nuestros días.

Producto de ello es loable reconocer también como parte de una realidad tangible y visible el papel que han adquirido las redes sociales y las diversas plataformas, lo que nos ha llevado muchas veces a replantearnos qué entendemos por privacidad e intimidad, producto de la ambivalencia constante entre lo público y lo privado. Qué está permitido y qué no, donde emerge la responsabilidad de los buscadores de internet, de los

proveedores, de terceros dueños de los contenidos de las páginas web, etc. Todo lo cual ha provocado que el derecho tuviera que poner su mano interventora para poder dirimir conflictos relacionados con derechos fundamentales en el mundo del ciberespacio.

Ello sumado a la comunicación e información, ambas a gran escala, se presenta un enorme desafío desde lo jurídico-constitucional, y desde lo político-electoral.

El uso de Big Data en procesos electorales ha transformado la forma en que se lleva a cabo el sufragio y la participación ciudadana. Este trabajo tiene por objetivo explorar cómo la recolección y análisis de grandes volúmenes de datos pueden influir en la toma de decisiones electorales, la segmentación de votantes y la optimización de campañas. A través de técnicas de minería de datos y aprendizaje automático, los partidos políticos pueden identificar patrones de comportamiento, preferencias y tendencias entre los electores, permitiendo una comunicación más efectiva y personalizada.

Además, se examina el impacto de las plataformas digitales y las redes sociales en la difusión de información electoral, así como los desafíos éticos y de privacidad que surgen con el uso de datos personales.

Para abordar estos objetivos, se adoptó una metodología cualitativa basada en el análisis documental de fuentes académicas, informes internacionales, normativas locales y estudios de caso. Se indaga especialmente en el fenómeno del microtargeting electoral, con énfasis en su aplicación concreta en campañas políticas, tanto en contextos internacionales como en la Argentina. Asimismo, se analiza el marco normativo vigente en el país, evaluando su adecuación frente a estas nuevas prácticas tecnológicas y comunicacionales. Esta aproximación busca ofrecer una mirada crítica e informada sobre los límites y posibilidades del uso de datos personales en procesos electorales democráticos.

II. El sufragio y el marketing electoral. Su evolución a lo largo de la historia

El sufragio es un derecho-deber de carácter político dirigido a formar la voluntad general del Estado. Es decir, es una manifestación de la voluntad individual que, junto con otras voluntades, constituye la voluntad general del Estado.

El pueblo, como titular y fuente originaria de la soberanía, el único medio esencial con el que cuenta para ejercer esta última es el sufragio. Solamente a través de él puede constituir a las autoridades de la Nación. Sin ella no existe el Estado. Por lo que no sólo estamos en presencia de un derecho sino también de un deber.

Si bien la organización constitucional argentina nació en 1853 y estableció la forma de gobierno representativa republicana, el sufragio no siempre estuvo contemplado constitucionalmente. De hecho, en el primer texto de 1853 no había un artículo que manifiestamente estableciera el sufragio ni sus características tal y como lo conocemos hoy.

Posteriormente, cuando se ejerció por primera vez el poder constituyente derivado, con la reforma de 1860 se incluyó el artículo 33 de los derechos no enumerados o implícitos y se asumió su inclusión en él por los principios de soberanía popular y forma republicana de gobierno.

Actualmente, la Constitución Nacional argentina contempla el sufragio en el artículo 37, con todas las características de la Ley Sáenz Peña – sancionada en 1912- y prevé igualdad entre hombres y mujeres para el acceso a los cargos públicos electivos, lo que va de la mano con la Ley N° 27.412 de paridad de género (sancionada en el año 2017).

No obstante, si bien tanto el sufragio como los partidos políticos constituyen elementos esenciales para el desarrollo del sistema democrático, subyace otro concepto fundamental: marketing electoral.

La palabra marketing procede del inglés, pero está integrada en cualquier lengua del mundo. Para entenderla se debe conocer primeramente lo que es “market”, que hace referencia al mercado.

La American Marketing Association ofrece una definición para este término, señalando que: *“El Marketing es una actividad, conjunto de instituciones y procesos para crear, comunicar, entregar y cambiar las ofertas que tengan valor para los consumidores, clientes, asociados y sociedades en general”*.¹ Así pues, el marketing intenta crear valor en diferentes

¹ PRIETO, L. (2021). *Evolución del marketing político en los últimos años*. [Tesis de grado, Universidad de Valladolid]. Repositorio institucional de la Universidad de Valladolid <https://uvadoc.uva.es/bitstream/handle/10324/51360/TFG-E-1232.pdf?sequence=1>

productos o marcas para que estas tengan un mayor nivel de satisfacción en los individuos que las adquieren.

Vinculado a lo político y electoral, la palabra marketing también ha adquirido un significado. Por ejemplo, para el autor Cotteret (1995) el marketing político es llevado a cabo por el candidato o por el partido a través de distintos medios, para tratar de cambiar la conducta y la opinión de los individuos por medio de la persuasión y, de ese modo, para obtener el mayor número de votos.

La finalidad del marketing político tiene que ver con mejorar la imagen pública del político, establecer una cierta conexión emocional para con el votante que permita influenciar la percepción política y, de ese modo, movilizar a los votantes.

En uno de los primeros países en los que se ha podido desarrollar el marketing político y electoral fue en Estados Unidos. Según el autor Maarek (1997), en base a tres características puntuales: el sistema electoral, la celebración de elecciones para seleccionar a todos los cargos públicos y el desarrollo de los nuevos medios de comunicación.

Una de las primeras elecciones en las que se llevó a cabo este tipo de prácticas la de Eisenhower en EEUU, a través de spots televisivos, y encuestas por correo. No obstante, fue a finales de los '70 y principios de los '80 cuando se consolidó la comunicación realizada por los partidos en la televisión, gracias a la tolerancia de la publicidad política.

En la actualidad el marketing político se centra principalmente en resaltar al líder político, debiendo éste tener claro y resaltar qué quiere ofrecer a los individuos, para que luego no haya una brecha insalvable entre lo prometido y lo cumplido al llegar al cargo público.

El marketing electoral es una parte del marketing político que se ejerce durante las campañas electorales de un determinado partido. Tiene una duración menor, equivalente a la duración de la campaña, debido a que su función es intentar posicionar al líder político en el poder.

Lo cierto es que el marketing político y electoral no se dio toda la vida de la misma manera. Así como ha ido evolucionando la sociedad toda y la forma de hacer política, el marketing en torno a la misma también.

En la antigüedad, las campañas políticas eran muy sencillas. Los partidos anunciaban sus propuestas a través de carteles en las ciudades, panfletos

y organizaban grupos de debate donde se invitaba al público a escuchar las ideas de los candidatos.

En la actualidad, los políticos pueden presentar sus ideas y propuestas a los votantes en cualquier momento, gracias a la tecnología y las diversas redes sociales. Se han adaptado a este nuevo entorno y lo aprovechan como una ventaja competitiva.

Los avances tecnológicos facilitan la recolección y análisis masivo de datos personales de los votantes. Los partidos y candidatos aprovechan esta información para segmentar a su audiencia en grupos específicos, enviando mensajes altamente personalizados. Esta táctica busca maximizar el impacto y la persuasión de las comunicaciones electorales.

Y esto fue factible gracias al Big data. El Big Data ha servido como herramienta en múltiples campos y con el tiempo también ha tenido cabida en el de la política utilizándose para obtener información acerca de los electores. El surgimiento de este nuevo fenómeno ayuda a los partidos a ofrecer de manera concisa aquello que quieren los individuos, gracias al mayor conocimiento acerca de sus preferencias.

Sin embargo, plantea preocupaciones legales y éticas, ya que la segmentación puede conducir a la manipulación de la opinión pública y la formación de burbujas informativas. Además, la falta de transparencia en la recolección y uso de datos puede socavar la confianza en el proceso electoral.

Analicemos en el próximo acápite el Big Data y su relación con los procesos electorales.

III. El Big Data y los procesos electorales

Hoy nos encontramos inmersos en una sociedad completamente digital, atravesada por la denominada Industria 4.0 o Cuarta Revolución Industrial, caracterizada por la integración de nuevas tecnologías de la información y comunicación (TICs).

Respecto de las TICs, Díaz Revorio agrupa diversos instrumentos que combinan tecnologías de las telecomunicaciones, de la informática y la radiodifusión, que en conjunto posibilitan la transmisión y recepción de información y comunicación como la telefonía fija, móvil, televisión, radio, Global Positioning System (GPS), los ordenadores, fax,

videoconferencias, Short Message Service (SMS), el correo electrónico, el chat y otros servicios de mensajería instantánea, siendo el internet la que tiene un indudable protagonismo.²

Para el desarrollo de estas ‘nuevas tecnologías’ de la información y comunicación, el ser humano creó vías que faciliten la implementación de estas en todo el mundo. Como muestra de ello, se desarrolló el internet a nivel mundial.

Dentro de las herramientas que se destacan también se encuentran el Big data, los algoritmos y la inteligencia artificial.

El Big Data refiere a la producción copiosa y voluminosa de datos que se da de forma espontánea³. A la utilización masiva de datos se la vincula con las 5 Vs: volumen, velocidad, variedad, veracidad y valor.

El volumen y la variedad tienen que ver con la gran cantidad de datos que se generan por segundo y la gran diversidad de fuentes de las que los mismos se obtienen producto de la interacción digital en los diferentes espacios que existen dentro de Internet. Por consiguiente, es posible hallar datos provenientes de redes sociales, tarjetas de débito/crédito, compras online, búsquedas en buscadores de internet, el Internet de las cosas (IoT), etc. Al respecto, González (2019) menciona que “...las personas producimos datos en tiempo real que se van almacenando y pueden ser analizados. Estos tienen la característica de que no reflejan las opiniones expresadas por las personas, sino que son “rastros” que dejamos involuntariamente en nuestros quehaceres cotidianos”⁴.

Con esta herramienta se obtienen datos de diversa índole, siendo la misma piedra angular que sirve de insumo para que –tecnologías mediante– sean conocidos e inferidos gustos, preferencias, intereses y

² Los derechos fundamentales y las nuevas tecnologías de la información y comunicación. file:///C:/Users/lucre/Downloads/DialnetLosDerechosFundamentalesYLasNuevasTecnologiasDeLaI-8328951.pdf

³ GIL DOMÍNGUEZ, A. (2023) “Constitucionalismo Digital”, 1° Ed., Ciudad Autónoma de Buenos Aires: Ediar.

⁴ GONZÁLEZ, F. 2019. Big data, algoritmos y política: las ciencias sociales en la era de las redes digitales Cinta moebio 65: 267-280 doi: 10.4067/S0717-554X2019000200267 https://pure.mpg.de/rest/items/item_3194120_1/component/file_3194121/content

problemáticas de la sociedad. El Big data como información almacenada y a la vez, el proceso que la haga útil.

Por su parte, la velocidad alude a la rapidez con que Big Data analiza los datos es muy alta. El proceso estudia y clasifica la gran variedad de datos en el momento en que son creados.

La veracidad apunta a determinar qué datos son reales y cuáles no. Como toda información, deben analizarse las fuentes y excluirse aquellos que no resultan veraces. Esta precisión en el análisis le da un valor agregado, fin primordial del Big Data, para que esas perspectivas ciertas y valiosas puedan ser utilizadas en el momento oportuno.

A todo este proceso se le suma el valor agregado que todo este procesamiento de información no sería posible sin la intervención de los algoritmos. Los algoritmos –esa secuencia de instrucciones que ofrecen una respuesta especial a cada problema específico (Joyanes Aguilar, 2008, p. 64)⁵– son los encargados de analizar patrones de conducta y extraer información significativa a partir de datos dispersos.

De acuerdo con Rey (2020) y Molinetti (2019), en el ámbito político, la utilización del Big Data se implementó en el año 2012 con la llegada de Barack Obama a la candidatura estadounidense. Desde entonces, el Big Data comenzó a ser utilizado ampliamente por los políticos, convirtiéndose en una herramienta de información sumamente poderosa.

De ello se desprende otro concepto sumamente relevante en lo que atañe al presente trabajo: microtargeting o micro-segmentación.

A continuación, analizamos de qué se trata y cuál es su influencia en el mundo electoral.

IV. El microtargeting como insumo del marketing electoral

El uso del Big Data no sería tan decisivo si no fuera por los múltiples usos que se le pueden asignar, como por ejemplo la segmentación y micro-segmentación, también conocida como microtargeting.

⁵ JOYANES AGUILAR, L. (2008). Fundamentos de programación: algoritmos, estructura de datos y objetos. McGrawHill.

Las innovaciones desarrolladas por la industria del Big Data han originado el denominado microtargeting y la propaganda electoral cognitiva. Esta nueva propaganda se denomina también propaganda inteligente debido a que se centra en los sesgos cognitivos, las características y las emociones de la ciudadanía para crear campañas propagandísticas especialmente diseñadas para las preferencias de cada uno de los votantes⁶.

El objetivo del microtargeting consiste justamente en agrupar a los electores en pequeños segmentos sincronizados con los distintos perfiles para así adaptar y dirigir los contenidos de la propaganda electoral y, de ese modo, conseguir que la publicidad personalizada alcance su objetivo e influya sobre la opinión de los votantes.

Actualmente es habitual observar que en cualquier búsqueda en internet posterior a visitar un comercio virtual nos aparezcan ofertas o anuncios de los productos que hemos visitado con anterioridad, este tipo de publicidad se realiza a partir de las denominadas cookies, como sostenía López Jiménez⁷. Las cookies son la forma de publicidad automatizada equivalente al microtargeting electoral, pero en la dimensión comercial. La gran diferencia entre estos microtargeting es que el electoral aprende de la interacción de la persona a la que tratará de influir por medio de argumentos emocionales que imitan sus intereses personales y sociales y con variantes de una campaña publicitaria amoldada a su perfil psicológico, en palabras de González de la Garza⁸.

Los destinatarios son aquellos votantes que están indecisos, aquellos a los que los partidos políticos saben que no han conquistado de modo seguro, por lo que, con esa información recabada, los candidatos pueden redirigir sus propuestas en pos de sumar dichos votos.

⁶ WOOLLEY, S., HOWARD, P. (2017). Computational Propaganda Worldwide: Executive Summary. *Oxford: Oxford UP*, 11, 1-15.

⁷ LÓPEZ, D. (2011). Las cookies como instrumento para la monitorización del usuario en la Red: la publicidad personalizada". *Revista de Ciencias Económicas*. 29 (2), 175-190.

⁸ GONZÁLEZ DE LA GARZA, L. (2018). La crisis de la democracia representativa. Nuevas relaciones políticas entre democracia, populismo virtual, poderes privados y tecnocracia en la era de la propaganda electoral cognitiva virtual, el microtargeting y el Big Data. *Revista de Derecho Político*. (103), 257-302. <https://doi.org/10.5944/rdp.103.2018.23203>.

Entender el microtargeting es provechoso para impactar con un mensaje personalizado a grupos selectos de personas y, de forma masiva, requiere de ciertos componentes esenciales para el éxito.

Debido a que el microtargeting actúa sobre individuos concretos, necesita apoyarse en el geomarketing para localizar votantes potenciales, combinando datos territoriales con información política. Esta herramienta facilita el desglose y análisis de grandes volúmenes de información, permitiendo así una geolocalización precisa de los distintos perfiles ciudadanos. A partir de los datos recogidos en encuestas y sondeos, se territorializa la información para obtener un mapeo más eficaz del electorado.

Luego, se clasifican los datos según variables como ubicación, edad, nivel socioeconómico y otras características relevantes. Este proceso permite detectar zonas o grupos con alto potencial estratégico. Aunque no todos los segmentos ni regiones presentan comportamientos homogéneos, agruparlos en micro-segmentos facilita la depuración de los datos y la construcción de modelos predictivos. Estos modelos asignan puntuaciones estimadas (scores) a cada individuo, lo que contribuye a delimitar con mayor precisión los objetivos de la campaña (Rivero, 2015).

Con esta base, se desarrollan contenidos y estrategias personalizados, muchas veces alejados de los métodos tradicionales. En contextos como el argentino, donde conviven las elecciones primarias (PASO) y las generales, este enfoque permite adaptar los mensajes a cada etapa del proceso electoral.

Una vez completado el análisis territorial y segmentado el electorado, se obtiene una visión más clara sobre qué comunicar, cómo hacerlo y a quién dirigir cada mensaje.

A continuación, se expondrán tres casos concretos donde el microtargeting fue determinante en campañas políticas.

V. Procesos electorales en que se implementó el Big Data

Sin pretender realizar una enumeración taxativa de los países que han empleado esta herramienta digital en el marco de procesos electorales, en el presente trabajo destacaremos tres: Estados Unidos –haciendo especial énfasis en el caso Cambridge Analytica–, Reino Unido y Argentina.

i. Estados Unidos

En relación con el primero de ellos, podemos decir que Estados Unidos fue uno de los países pioneros en implementar el uso de la herramienta digital Big Data en el marco de la campaña electoral de Barack Obama en el año 2012. En aquella oportunidad, Obama optó por emplear una combinación de la base de datos analítica HP Vertica MPP junto con modelos predictivos, con el objetivo de aumentar su competitividad frente a los demás postulantes.

En otra oportunidad, en el año 2017, fue empleado el Big Data por el candidato Donald Trump, quien recurrió a la consultora Cambridge Analytica.

Cambridge Analytica fue una compañía privada británica que combinaba la minería de datos y el análisis de datos con la comunicación estratégica para el proceso electoral. La empresa fue creada en 2013, rama de la casa matriz Strategic Communication Laboratories (SCL), para participar en la política estadounidense⁹. Adquirió auge en 2018 al verse involucrada en el llamado escándalo Facebook-Cambridge Analytica.

En esa ocasión la empresa trabajó para la campaña electoral de Donald Trump. De acuerdo con las revelaciones publicadas por The Guardian y The New York Times, Cambridge Analytica recolectó millones de datos de usuarios estadounidenses de la red social mediante un software y un esquema capaz de predecir e influenciar a los votantes. Y lo hizo sin autorización, a través de una aplicación de encuestas llamada This Is Your Digital Life.

Los resultados de la encuesta se integraron con la actividad de los usuarios en Facebook, y diversos algoritmos facilitaron la creación de campañas segmentadas de alta precisión dirigidas a aproximadamente dos millones de usuarios estadounidenses durante la campaña presidencial de Donald Trump, que lo llevaron a la presidencia en 2017.

⁹ Wikipedia (s.f.). *Cambridge Analytica*. Recuperado de https://es.wikipedia.org/wiki/Cambridge_Analytica

ii. Reino Unido de Gran Bretaña

Otro país en el que se ha empleado es en el Reino Unido de Gran Bretaña. En el año 2016 la campaña a favor del Brexit utilizó técnicas de microtargeting basadas en Big data. Analizaron datos demográficos y de comportamiento para dirigir anuncios específicos a diferentes grupos de votantes, influyendo en la decisión del referéndum.

En ese referéndum, el SCL Group colaboró con las campañas políticas Leave.eu (relacionada con el partido de extrema derecha UKIP) y Vote Leave (relacionada con el partido conservador) para que el Reino Unido abandonara la Unión Europea, por medio de sus empresas subsidiarias Cambridge Analytica y AggregatedIQ (Cadwaladr 2017b).

Por un lado, se llevó a cabo una campaña de microtargeting dirigida a votantes indecisos que podrían optar por la salida del Reino Unido (Wylie 2019). El análisis de Big data identificó dos preocupaciones principales en este grupo: la justicia social y el trato a los extranjeros de la Commonwealth. La campaña Vote Leave lanzó Be Leave, enfocándose en temas como la igualdad de trato a inmigrantes, la discriminación hacia ciudadanos fuera de la UE y la protección del medioambiente.

Por otra parte, se realizó una gran inversión en una campaña de distorsión informativa mediante la difusión de fake news en redes sociales, enfocándose en inmigración y economía. En cuanto a la inmigración se afirmaba que la permanencia en la Unión Europea aumentaba la llegada de trabajadores poco cualificados y que la posible inclusión de Turquía generaría una avalancha de refugiados. En economía, se difundieron noticias evidenciando un costo millonario por pertenecer a la UE.

Esta repetición masiva de afirmaciones generó un clima de rabia que favoreció a las candidaturas del leave.

iii. Argentina

En el caso de Argentina, se dice que se recurrió a esta herramienta para las elecciones de 2015 en las que Mauricio Macri llegó a la presidencia de la Nación¹⁰.

¹⁰ SEIBERT, T (2021) "Big Data y Democracia ¿La utilización del Big Data representa una amenaza para el estado de democracia? Análisis de la campaña electoral del PRO 2015, XIV Jornadas de Sociología. Facultad de Ciencias Sociales, Universidad de Buenos Aires, Buenos Aires.

El PRO fue el primer partido político que empleó en Argentina la propaganda por medio de las redes sociales.

Dicho partido desarrolló una campaña electoral que se dividió en dos ámbitos: online y offline, pero coordinados entre sí. Al respecto, según lo expresado por sus entrevistados, Milánes¹¹ afirma que la división de la campaña entre lo digital y lo territorial fue “la clave del éxito de la campaña presidencial de Cambiemos”.

En cuanto a la campaña electoral online la red social protagonista de ese entonces fue Facebook, no sólo determinante por la cantidad de usuarios/as en Argentina, sino también la posibilidad que brindaba la plataforma de difundir publicidad segmentada. Esto fue clave en el sentido que el PRO era un partido político que primordialmente había nacido en la ciudad de Buenos Aires y necesitaba tener la mayor extensión territorial posible.

El uso de Facebook se complementó con la plataforma SpreadShout, la cual permitió que los usuarios afines al candidato se convirtieran en influenciadores que pudieran servir para multiplicar y potenciar el cambio.

También se utilizó Whatsapp, sumado a datos recolectados en la propia página oficial y el famoso “timbreo” –campaña offline-, y se valió del neuromarketing “...herramienta (...) para incrementar la empatía por parte de los votantes y, en definitiva, conseguir la concreción de su fin último: maximizar la posibilidad de ser electo”¹².

Esto permitió conocer gustos, necesidades, preferencias, problemas, deseos y conductas y lograr éxito en la campaña, depositando al candidato Macri en la presidencia de la Nación por el período 2015-2019.

Este 2025 Argentina atraviesa un año electoral y es clave considerar cómo influye el uso de datos personales a través de tecnologías digitales.

¹¹ MILANES, M. (2018). Microtargeting en elecciones. Análisis exploratorio: 1º caso de estudio | PRO 2015-2017. Asociación por los Derechos Civiles (ADC).

¹² DENING, K. I., & Salas, M. F. (2017). Neuromarketing político aplicado a la campaña presidencial de Mauricio Macri. Buenos Aires.

Gracias al Big Data, es posible monitorear redes sociales y portales, recolectar opiniones, filtrarlas y clasificarlas automáticamente según estén a favor o en contra de un tema. Esto permite a los candidatos ajustar estrategias y predecir resultados. Además, surgen los *chatbots*, programas que simulan usuarios reales para influir en conversaciones online, promoviendo o desprestigiando candidatos. Estos últimos, en campañas, buscan consolidar una narrativa favorable y pueden actuar como “influencers” digitales.

Los equipos de campaña ya no sólo necesitan expertos políticos, sino también analistas de datos. Las herramientas digitales permiten conocer mejor al electorado y dirigir mensajes personalizados, especialmente a votantes indecisos. En esta era, quien sepa usar los datos tendrá ventaja, aunque los ciudadanos deben seguir siendo críticos y responsables al informarse y decidir su voto.

iv. ¿Cuáles son los riesgos y/o desafíos que se presentan desde el ámbito político, social y ético con el uso del microtargeting?

Como se desprende de los casos ut supra referenciados, el uso del microtargeting como insumo electoral presenta retos, desafíos y hasta si se quiere riesgos tanto en el ámbito político como social y ético.

Bajo esa línea se puede mencionar como riesgo principal se presenta en la manipulación política dado que permite a los postulantes enviar mensajes direccionados a aquel público indeciso, valiéndose de datos relativos a sus gustos, preferencias e intereses. Los mensajes se realizan apelando a las emociones, miedos, prejuicios específicos, manipulándose las decisiones de voto sin promover un debate racional.

Eso también repercute en la deliberación política dado que no hay un mensaje común, sino una visión más bien fragmentada, lo que puede también hacer recaer a los partidos políticos en mensajes contradictorios atentado contra su propia propuesta para alcanzar el gobierno.

Estos riesgos han sido objeto de sanción de normativas a nivel internacional con el fin de regular el uso ético del Big Data como, por ejemplo, el Reglamento de la Unión Europea N° 900/2024¹³.

¹³ Reglamento Europeo 2024/900 del Parlamento Europeo y del Consejo. (2024).

Este reglamento tuvo como objetivo garantizar la transparencia y evitar la manipulación política, estableciendo obligaciones y responsabilidades para los proveedores de propaganda política dentro de la Unión Europea, transparencia en los anuncios y la información sobre quién los financia.

Otro riesgo es el relativo al manejo y uso que se hace de los datos personales. Porque se trata de grandes volúmenes de datos (incluyendo datos personales sensibles) y porque muchas veces esos datos se obtienen a través de prácticas confusas, opacas y poco transparentes.

Por su parte, otra cuestión no menos importante es la amenaza latente de caer en discriminación, dado que los algoritmos utilizados pueden producir sesgos discriminatorios (por edad, por género, por nivel socio-económico, etc.), por lo que algunos grupos o sectores podrían resultar excluidos o no considerados electoralmente “valiosos”. Esto también fue objeto de regulación en el reglamento antes mencionado: la prohibición de segmentación en sectores sensibles.

También a nivel europeo se sancionaron en 2024 Directrices sobre protección de datos y autenticación electoral, cuya finalidad fue limitar el uso indebido de datos biométricos y electorales por autoridades y prohibir su uso por partidos políticos o terceros; y, por otra parte, establecer transparencia en evaluaciones de impacto de derechos humanos al contratar tecnología electoral.

En el marco de la OEA se sancionó la Guía para garantizar la libertad de expresión frente a la desinformación deliberada en contextos electorales¹⁴, elaborada por la Relatoría Especial para la Libertad de Expresión (RELE) en coordinación con el Departamento de Cooperación y Observación Electoral de la OEA.

Allí se establecieron recomendaciones específicas para cada actor sobre cómo prevenir y contrarrestar la desinformación electoral. Define la desinformación deliberada cuando hay difusión masiva de información falsa existiendo intencionalidad de engañar al público, conociendo lógicamente el emisor la falsedad de la información. Todo esto teniendo como eje central los derechos humanos. Además, emite una lista con

¹⁴ Comisión Interamericana de Derechos Humanos. (2019). *Guía para garantizar la libertad de expresión frente a la desinformación deliberada en contextos electorales*. Organización de los Estados Americanos. Recuperado de https://www.oas.org/es/cidh/expresion/publicaciones/Guia_Desinformacion_VF.pdf

recomendaciones para los Estados y para las autoridades electorales con la finalidad de fortalecer tanto la libertad de expresión como la integridad de los procesos electorales.

VI. El Big Data y el Derecho argentino vigente

Si bien la recolección de datos genera un gran debate en cuanto a su legalidad, también entran en consideración las fuentes de las que es extraída esa información.

Analicemos en este acápite: el Big Data y el microtargeting ¿colisionan con la normativa argentina vigente en materia de protección de datos personales?

La recolección y análisis de datos plantea preocupaciones sobre la privacidad y el uso ético de la información. La legislación debe abordar cómo se utilizan los datos de los ciudadanos y proteger su información personal.

En la mayor parte de las oportunidades la información es tomada de las diversas huellas digitales que el sujeto va dejando primordialmente en las redes sociales (Facebook, Instagram, Twitter, Tiktok), aunque también las que deja en las búsquedas en buscadores de internet, como Google, o Youtube, entre otras.

La Ley de Protección de Datos Personales (en adelante la LPDP), en su artículo 2 enumera cuáles son los datos personales y, de modo taxativo, cuáles los datos personales sensibles. Entre estos últimos coloca a las opiniones políticas.

Complementariamente, en el artículo 7 del mismo cuerpo legal, se prevé expresamente la prohibición de crear registros que contengan datos sensibles, con excepción de la Iglesia Católica, y en el tema específico que nos convoca, las asociaciones políticas respecto de sus afiliados.

La LPDP es clara en cuanto a la rigidez en el tratamiento de datos personales sensibles –en las que ingresan las opiniones políticas–, pero no menos cierto es que la propia persona es la que en mayoría de los casos rompe con esa barrera entre lo público y lo privado, exponiendo sus convicciones íntimas ante miles y miles de personas.

El famoso concepto de “privacidad online” que por momentos pareciera responder más a “publicidad online”. La realidad evidencia que el com-

portamiento de los sujetos de internet y las redes que, básicamente, se centra en exhibir y compartir su intimidad y subjetividad, pone en jaque ciertos aspectos tradicionalmente protegidos por el derecho a la privacidad.

Aquí me parece sumamente interesante diferenciar intimidad de privacidad. La intimidad responde a aquellos actos que el ser humano lleva a cabo en su morada, refiere a una zona espiritual más reservada, interna y personal; en cambio, los actos privados son aquellos que pueden ser ejercidos en un ámbito reservado como así también ser expuestos en la vida pública.

Esto último sucede con los datos expuestos en redes sociales, dado que más allá que cada usuario los comparta con sus “amigos” (en caso de Facebook) o “seguidores” (en los supuestos de Instagram, Twitter o Tiktok) los mismos se reproducen velozmente de modo tal que la persona pierde dimensión del alcance que la misma tiene. Con lo cual, si esos datos luego son captados por Big Data, en principio, podríamos decir que no existiría infracción a la normativa vigente: la persona en ningún momento es coaccionada a brindarla, sino que lo hace de modo consciente, en el marco de su autodeterminación informativa, vale decir, sabiendo qué, cómo y hasta dónde darse a conocer con terceros (art. 43 3er párrafo de la Constitución Nacional). Expone voluntariamente su pensamiento y opinión política.

Por otra parte, se suscitan dos cuestiones más a tener presentes. En primer lugar, que no se busca identificar específicamente la preferencia política de estos sujetos en particular –porque reitero, generalmente se trata de sujetos indecisos– sino todo tipo de gustos, preferencias e intereses. La información que se recaba responde a un universo mucho más amplio, de modo tal de dirigir y adaptar con la mayor probabilidad de éxito la propuesta electoral y conquistar cada uno de esos votos. Por ello, cuanto más se conozca del electorado vacilante, más efectiva resultará la medida. No se pretende identificar a una persona en particular ni diseñar una propuesta electoral personalizada específicamente para ella.

La segunda cuestión a tener presente que, si bien la información se extrae de las cuentas de múltiples internautas, se persigue también una finalidad estadística –la cual sí es legal y está permitida–, que sirve para conocer qué porcentaje del padrón hay que conquistar, partiendo de la base de conocer aquello que no termina de generar convicción en esas

personas a través de las ideas y raciocinios que manifiestan, sin que necesariamente sean identificados los titulares de esos datos. Hasta incluso podría decirse que no requieren consentimiento del titular por recabarse para funciones propias del Estado –artículo 5 inciso b) de la LPDP–.

De esta manera, pareciera caer por tierra cualquier tipo de argumento que sustente la transgresión de la ley de protección de datos en virtud de ser datos sensibles.

Sin perjuicio de ello y, conforme lo previsto en el Anexo I aprobado por la Resolución N° 86/2019 de la Agencia de Acceso a la Información Pública, los *“datos personales publicados en redes sociales, foros o plataformas web de fácil acceso o acceso irrestricto, también están alcanzados por los principios fundamentales de la Ley N° 25.326, por lo que deben adecuarse a los principios (...)”*, como así también *“los datos personales que vayan a ser utilizados para el envío de propaganda electoral tales como, el correo electrónico, la cuenta de una red social, de un servicio de mensajería instantánea u otros similares deberán haber sido obtenidos lícitamente, amparados en alguna de las bases legales contenidas en los arts. 5 o 7 de la Ley N° 25.326”*¹⁵.

Sería provechoso poder crear una norma específica que permita regular el uso del Big Data en el marco de procesos electorales, donde se definan los términos esenciales, se respeten los principios rectores en materia de protección de datos, prohibición de uso de dichos datos sin expreso consentimiento de las personas, obligación de anonimización o seudonimización cuando sea ello factible, y regulación expresa para datos que se obtienen de las redes sociales.

Asimismo, sería interesante lograr implementar la transparencia algorítmica bajo tres pilares fundamentales: a) obligatoriedad de informar cuando se utiliza un sistema automatizado de datos para segmentar o personalizar mensajes político-electorales; b) derecho de los ciudadanos a conocer cómo funcionan los algoritmos que inciden en la experiencia electoral y c) realización de auditorías externas obligatorias de los algoritmos utilizados por los partidos políticos, consultoras, plataformas, etc.

15 Ver cláusulas 7 y 8 file:///C:/Users/lucre/Downloads/anexo_5745822_1.pdf

En un mismo sentido, podría establecerse como órgano de control la Cámara Electoral- institución por excelencia a cargo de los comicios- con el objeto de supervisar el uso de las herramientas tecnológicas del propio proceso y, de forma complementaria, la Agencia de Acceso a la Información Pública para todo lo relativo a la protección de datos personales y acceso a la información sobre los algoritmos.

En un mismo orden de ideas, también considero que, de crearse una norma marco que regule el uso del Big data en los procesos electorales, debería contemplarse la responsabilidad de los partidos políticos. Así como estos deben dar cuentas del origen y destino de los fondos porque los sostiene el propio Estado –artículo 38 de la Constitución Nacional- también hace a su responsabilidad la rendición de cuentas en el uso de los algoritmos e información de los propios ciudadanos, en caso de hacer uso de ellos.

No obstante, entiendo quizás que el foco además de ponerlo en lo legal habría que ponerlo en lo ético. Entonces cabe preguntarnos: ¿es ético recurrir a este tipo de herramientas como ejes que direccionan los procesos electorales? ¿Es ético direccionar propagandas políticas para generar la convicción interna de cada votante a partir de relatos que construyen los propios candidatos, en función del análisis e investigación de los gustos, preferencias, inquietudes y demandas de la población? Quizás no sea ilegal porque la recolección de datos se ajuste a la normativa vigente, pero: ¿es ético?

VII. Conclusión

A modo de cierre, podemos decir que el uso de Big data en los procesos electorales representa una herramienta poderosa que puede transformar la forma en que se llevan a cabo las campañas y se entiende el comportamiento del electorado. Sin embargo, su implementación también plantea desafíos significativos relacionados con la privacidad y la ética en el uso de esa información.

En ese sentido, en Argentina se vuelve fundamental avanzar en la elaboración de una norma específica que regule el uso de Big Data y herramientas algorítmicas en los procesos electorales, con el objetivo de garantizar su aplicación ética, transparente y respetuosa de los derechos ciudadanos.

Asimismo, se debe fomentar una cultura de educación cívica que empodere a los votantes, permitiéndoles tomar decisiones informadas y críticas, evitando de esa manera que el uso excesivo de estas herramientas tecnológicas termine deshumanizando el proceso electoral y la participación ciudadana no termine reflejando la verdadera voluntad general del Estado, que es –en definitiva– el verdadero objetivo del sufragio.

El equilibrio entre innovación y responsabilidad será clave para asegurar que el uso de Big data fortalezca, en lugar de socavar, los principios democráticos. Solo así se podrá aprovechar su potencial para mejorar la calidad de la democracia y la participación ciudadana, reconociendo que el poder recae en el pueblo y no en los algoritmos.

Sistemas expertos en el Poder Judicial de Perú: El caso de Amauta Pro

Gianfranco Mejía Trujillo*

Resumen.- El presente artículo analiza a los Sistemas Expertos como parte de los sistemas de Inteligencia Artificial que buscan brindar insumos relevantes para la toma de decisiones. Para ello, se hace referencia al caso de Amauta Pro, el cual fue desarrollado recientemente por el Poder Judicial del Perú, a fin de explicar sus características, beneficios, limitaciones, criterios de éxito y oportunidades de mejora en su implementación.

Palabras clave.- Sistemas Expertos – Inteligencia Artificial – Amauta Pro – Poder Judicial – Toma de Decisiones – Interoperabilidad – Transparencia – Razonamiento Jurídico.

Abstract.- This article analyzes Expert Systems as part of Artificial Intelligence systems that seek to provide relevant input for decision-making. To this end, we refer to the case of Amauta Pro, which was recently developed by the Peruvian Judiciary, to explain its characteristics, benefits, limitations, success criteria, and opportunities for improvement in its implementation.

Keywords.- Expert Systems - Artificial Intelligence - Amauta Pro – Judiciary - Decision-making – Interoperability – Transparency - Legal Reasoning.

* Abogado especializado en Gestión Pública, Regulación, Derecho Administrativo e Inteligencia Artificial. Posee una experiencia de más de 20 años en el sector público peruano, habiendo ejercido diversos cargos directivos. Es Director del Programa Especializado en Regulación de la Inteligencia Artificial (Universidad Peruana de Ciencias Aplicadas) y miembro del Observatorio Sector Público e Inteligencia Artificial (OspIA) y del CAIDP Fall 2024 AI Policy Clinic Research.

I. Introducción

El nuevo paradigma sociocultural quebranta los elementos del tiempo, lugar y espacio conocidos en la narrativa de la humanidad. Este panorama ha derivado del fortalecimiento

El Poder Judicial de Perú enfrenta constantemente muchos retos para poder mejorar la prestación de sus servicios a la ciudadanía, reflejados principalmente en la solución adecuada y oportuna de las controversias jurídicas que son puestas a consideración de sus operadores jurídicos: los jueces.

La demora y la falta de predictibilidad de las decisiones judiciales, entre otros aspectos negativos, conllevan una serie de costos que son asumidos por los ciudadanos y también por los operadores jurídicos de otras entidades públicas, generándose una situación que perjudica a todos los involucrados y, por ende, a una adecuada administración de justicia.

Con el desarrollo progresivo de la noción de un Gobierno Digital en nuestro país, se vuelve importante considerar la pertinencia y la utilidad de emplear tecnologías digitales para mejorar la prestación de servicios de las entidades públicas, como ocurre con el caso del Poder Judicial.

En esa línea, es posible evaluar el empleo de una tecnología que, si bien se ha desarrollado desde hace varias décadas, en los últimos años ha tenido un gran auge: la Inteligencia Artificial (IA), la cual posee diversas características que pueden brindar mejoras a la prestación de servicios por parte de las entidades públicas, las que se reflejarán en beneficios concretos para los ciudadanos.

Considerando lo indicado, en este artículo revisaremos la aplicación de un sistema de IA en el Poder Judicial de Perú, denominado Amauta Pro, bajo la figura de lo que se conoce como un Sistema Experto (SE) cuyos detalles se expondrán en las siguientes líneas a fin de comprender cuál es su naturaleza, cómo opera, cómo se gestó su desarrollo en el país, cuáles son sus ventajas y limitaciones, así como qué criterios se pueden tomar en cuenta para asegurar el éxito y la mejora continua en su implementación.

II. Inteligencia Artificial y Sistemas Expertos

La IA es un campo amplio de conocimientos que aborda diversos aspectos vinculados con el desarrollo y funcionamiento de sistemas que, sobre la base del procesamiento de datos y el empleo de algoritmos,

ofrecen productos basados en distintas técnicas que reflejan diversos niveles de adaptabilidad y autonomía que tienden a asemejarse a los del cerebro humano, participando en menor o mayor medida en la toma de decisiones humanas.

El referido campo de conocimientos vinculado con la IA se puede dividir en dos grandes áreas. El primero de ellos se vincula con el desarrollo que estamos apreciando en los últimos años, meses y días, como por ejemplo el caso de la IA Generativa o los Agentes de IA, entre otros.

Esta área se vincula con la mejora continua de la toma de decisiones mediante el aprendizaje probabilístico, incluyendo a las técnicas conocidas como el aprendizaje automático (*machine learning*) y el aprendizaje profundo (*deep learning*), entre otros, resaltándose la importancia de la capacidad computacional, el incremento de la recolección de datos y demás aspectos vinculados¹.

La segunda área, que no se destaca mucho en este último período, consiste en el desarrollo de sistemas de IA basados en el conocimiento, dentro de los que se encuentran los Sistemas Expertos (SE), los cuales funcionan sobre la base de reglas y axiomas predeterminados, empleando reglas programadas y lógica formal para razonar en diversos ámbitos de conocimiento especializados². Los analizaremos con más detalle a continuación.

III. Sistemas Expertos

Los SE existen desde hace varias décadas, formando parte de los primeros esfuerzos por demostrar los avances del desarrollo de los sistemas de

¹ ZAFAR, A. (2024). Balancing the scale: navigating ethical and practical challenges of artificial intelligence (AI) integration in legal practices. *Discover Artificial Intelligence*, pp. 3. El citado autor indica: "AI technology may be broadly divided into two areas. (...) The second category consists of technologies that continuously improve decision-making through probabilistic learning. This category, which encompasses machine learning and deep learning approaches, is driven by improved computer processing power, lower prices for digital storage, and increased data collection".

² *Idem.*, El citado autor indica: "AI technology may be broadly divided into two areas. The first category includes knowledge-based systems, or expert systems, which function by inferring behaviour given a set of axioms. These systems use programmed rules and formal logic to reason in certain domains".

IA en el siglo pasado. Sin embargo, podemos afirmar que en el ámbito jurídico empezaron a tomar forma en la década de 1980 del siglo pasado, siendo importante la labor que en el ámbito teórico y práctico desarrolló el académico Richard Susskind, cuyos artículos reseñaremos a lo largo del presente artículo.

El año 1986, Susskind publicó uno de los primeros artículos de investigación sobre los SE en el Derecho, definiéndolos como programas computacionales que son construidos con el apoyo de seres humanos expertos, de manera que pueden funcionar al nivel (y a veces de mejor manera) que dichos expertos en algunos campos de conocimiento, siendo usados como un apoyo de alto nivel intelectual (asistentes inteligentes) para sus usuarios³.

Una definición mucho más actual complementa a la anterior, resaltando que los SE están compuestos por: (i) una base de datos de conocimientos que contiene información relevante sobre la materia involucrada en el sistema y, (ii) un motor de inferencia que aplica las reglas de la lógica y la probabilidad a la base de conocimientos para plantear conclusiones a sus usuarios⁴.

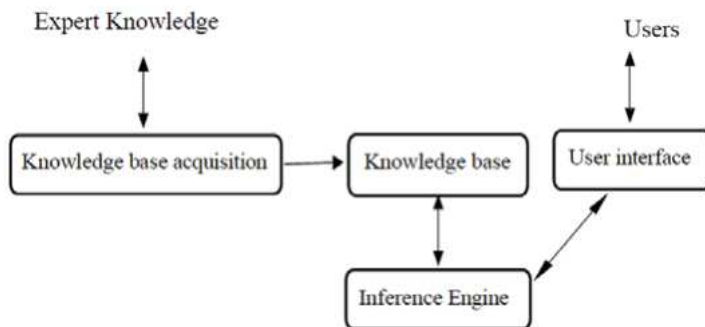
Lo indicado se puede graficar de la siguiente manera⁵ (ver gráfico en la siguiente página).

De acuerdo con el gráfico expuesto, los SE requieren para su funcionamiento iniciar con la adquisición de una base de conocimientos (*knowledge base acquisition*) derivada de los expertos (*experts knowledge*),

³ SUSSKIND, R. (1986). Expert Systems in Law: A Jurisprudential Approach to Artificial Intelligence and Legal Reasoning. *Modern Law Review*, pp. 172. El citado autor indica: "Expert systems are computer programs that have been constructed (with the assistance of human experts) in such a way that they are capable of functioning at the standard of (and sometimes even at a higher standard than) experts in given fields. They are used as high-level intellectual aids to their users; this explains their alternative epithet: intelligent assistants".

⁴ JURS, A. & DEVITO, S. (2024). Machines Like Me: A Proposal on the Admissibility of Artificially Intelligent Expert Testimony, *Pepperdine Law Review*, pp. 616. El citado autor indica: "An expert system is composed of a database (the "knowledge base") containing relevant information about the subject matter of the system and the program (the "inference engine") that applies the rules of logic and probability to the knowledge base to draw conclusions".

⁵ *Idem*.



constituyéndose dicha base en la de los conocimientos del sistema (*knowledge base*), de manera que los datos involucrados sean procesados en el motor de inferencia (*inference engine*) y derivados a la interfaz de usuario (*user interface*), a fin de que los usuarios (*users*) puedan apreciar los insumos ofrecidos por el SE.

Como se puede apreciar de estas definiciones y de la descripción de su funcionamiento, los SE tienen un enfoque muy concreto de actuación, buscando constituirse en un apoyo importante para la toma de decisiones de los seres humanos en ámbitos que requieren de un conocimiento muy especializado, como ocurre con los diagnósticos de enfermedades o el análisis legal, entre otros, constituyéndose en asistentes inteligentes que aportan insumos relevantes considerando la base de conocimientos que les sirven de sustento.

Una de las principales características que se resaltan de los SE consiste en su transparencia, en atención a que, tomando en cuenta que su funcionamiento radica principalmente en su base de conocimientos y el motor de inferencia que son determinados y controlados por los seres humanos, es más factible conocer de manera detallada el proceso por el cual se generan los insumos por parte de los SE, y así poder explicar con mayor claridad cómo contribuyeron dichos insumos con la decisión final tomada por la seres humanos⁶.

⁶ SUSSKIND, R. (1986). Expert Systems in Law: A Jurisprudential Approach to Artificial Intelligence and Legal Reasoning. Modern Law Review. El citado autor indica: "Expert systems are usually: (1) transparent, which means that they can generate explanations of the lines of reasoning that lead them to their conclusions (...)"

Lo indicado permite que los SE sean considerados como sistemas de “caja abierta o blanca” (*open or white box systems*⁷), en contraste con los sistemas que son catalogados como “cajas negras” (*black-box systems*), los cuales enfrentan altos niveles de opacidad que afectan a su transparencia, lo que se presenta con mayor intensidad en los sistemas de IA que se están desarrollando con mayor intensidad en este último período (IA Generativa, Agentes de IA, entre otros) al requerir de una gran cantidad y diversidad de datos y operar mediante el empleo de algoritmos de mucha complejidad, entre otros aspectos.

Además de la transparencia, los SE poseen las siguientes características: (i) son heurísticos, al razonar sobre la base del conocimiento formal e informal que refleja la especialización en un ámbito determinado y, (ii) son flexibles, al poseer la habilidad de permitir, sin mayor dificultad, que se realicen modificaciones a sus bases de conocimiento cuando sea pertinente⁸.

Las características de los SE que han sido descritas, permiten brindar mayores alcances sobre su funcionamiento, así como respecto de los posibles beneficios y limitaciones que se puedan presentar, lo que nos servirá para poder tomarlas en cuenta al hacer referencia en el próximo acápite al caso de un SE implementado por el Poder Judicial de Perú: el sistema de IA Amauta Pro.

⁷ JURS, A. & DEVITO, S. (2024). *Machines Like Me: A Proposal on the Admissibility of Artificially Intelligent Expert Testimony*, Pepperdine Law Review. El citado autor indica: “As we have seen, as expert systems become more sophisticated, they become more difficult to understand (...). Despite these concerns, we should recognize that expert systems are transparent and explainable, and therefore are, in principle, open-box systems”.

⁸ SUSSKIND, R. (1986). *Expert Systems in Law: A Jurisprudential Approach to Artificial Intelligence and Legal Reasoning*. Modern Law Review. El citado autor indica: “Expert systems are usually: (...) (2) heuristic, by which is meant they reason with the informal, judgmental, experiential and often procedural knowledge that underlies expertise in a given field (as well as with the more formal knowledge of the domain in question); and (3) flexible, a term that refers to the ability of these systems to allow, without any great difficulty, modifications to their knowledge bases, that is, to their stores of knowledge”.

IV. El Sistema Experto Amauta Pro del Poder Judicial del Perú

i. Marco normativo aplicable

En el Perú no se cuenta con un marco normativo específico sobre el uso de la IA en general por parte de las entidades públicas, por lo que no existen criterios jurídicos aplicables de manera concreta a su uso por parte del Poder Judicial. Tampoco existen guías o lineamientos sobre el particular.

Si bien desde julio de 2023 se encuentra vigente la Ley 31814, Ley que promueve el uso de la IA en favor del desarrollo económico y social del país, su contenido es muy genérico y no establece criterios concretos sobre su uso por parte del sector público, por lo que será necesario esperar a su reglamentación que todavía sigue pendiente para poder tener mayores alcances al respecto.

No obstante, existen referencias internacionales como los casos del Reino Unido y Colombia, países que recientemente emitieron disposiciones que regulan el uso de la IA por parte de sus cortes judiciales.

Reino Unido publicó en diciembre de 2023 su Guía para titulares de cargos judiciales, la cual fue actualizada en abril de 2025. Si bien se centra principalmente en el uso de la IA Generativa, sus pautas se aplican a cualquier sistema de IA a ser empleado por los jueces como parte de su labor, tales como: entender a la IA y sus aplicaciones, defender la confidencialidad y la privacidad, garantizar la responsabilidad y la precisión, estar atento a los sesgos, mantener la seguridad, asumir la responsabilidad y, ser consciente de que los usuarios de las Cortes pueden haber usado sistemas de IA⁹.

En diciembre de 2024, Colombia publicó sus Lineamientos para el uso y aprovechamiento respetuoso, responsable, seguro y ético de la IA en la Rama Judicial, los cuales, al igual que el documento del Reino Unido, a pesar de enfocarse en el uso de la IA Generativa, establece principios para el uso de cualquier sistema de IA en el ámbito judicial, como los siguientes: primacía de los derechos fundamentales, regulación ética, adecuación a buenas prácticas, no sustitución de la responsabilidad

⁹ Courts and Tribunals Judiciary (2025). Artificial Intelligence Guidance for Judicial Office Holders. United Kingdom.

humana, idoneidad, verificación humana, transparencia, prevención de riesgos, entre otros¹⁰.

Cabe resaltar que, tomando en cuenta las características positivas de los SE respecto de sus niveles de transparencia de su funcionamiento y claridad de resultados, éstos pueden ajustarse a los criterios establecidos en documentos internacionales sobre la materia publicados en Reino Unido y Colombia.

ii. Precisiones preliminares

Es necesario destacar que en el Perú no se cuenta con el nivel de transparencia algorítmica suficiente para poder contar con mayores datos e información más detallada sobre el funcionamiento de sistemas de IA en general empleados por el sector público, lo que no sólo restringe la posibilidad de profundizar en su estudio sino también puede afectar a los derechos de los ciudadanos involucrados en su funcionamiento¹¹.

Considerando lo indicado, es necesario precisar que los detalles sobre el sistema de IA Amauta Pro (en adelante, Amauta) se basarán estrictamente en los datos y la información contenidos en las resoluciones administrativas emitidas por la Corte Superior de Justicia de Lima Norte (en lo sucesivo, la Corte), por lo que el análisis de su funcionamiento se realizará sobre la base de dichos insumos.

iii. Amauta

La historia de Amauta comienza el 18 de agosto de 2023, con la emisión de la Resolución Administrativa 1086-2023-P-CSJLIMANORTE-PJ por parte de la Corte en cuyo considerando quinto se resaltó que:

¹⁰ Consejo Superior de la Judicatura (2024). Lineamientos para el uso y aprovechamiento respetuoso, responsable, seguro y ético de la inteligencia artificial en la Rama Judicial. Colombia. https://actosadministrativos.ramajudicial.gov.co/GetFile.ashx?url=%7E%2FApp_Data%2FUpload%2FPCSJA24-12243.pdf

¹¹ Para mayores alcances sobre esta materia, puede revisarse: Mejía, G. (2025). Transparencia Algorítmica y procedimiento administrativo: la importancia de la explicabilidad de la inteligencia artificial. Libro de ponencias del V Congreso Internacional de Derecho: Los Retos Multidisciplinarios de la Administración Pública de la Universidad San Ignacio de Loyola, Tirant Lo Blanch.

(...) se acordó nombrar al software de soporte profesional para la labor del Juez de Familia, un asistente jurisdiccional con inteligencia artificial denominado “Amauta PRO”, en referencia al gran sabio y consejero del imperio de los Incas, que enseñaba tanto leyes como matemáticas (...) ¹².

En el artículo primero del extremo resolutivo de la resolución indicada, se dispuso el desarrollo del asistente jurisdiccional con inteligencia artificial denominado: “Amauta Pro”, con la finalidad de asistir al Juez en la clasificación del riesgo y la redacción de los proyectos de medidas de protección en el sistema de prevención de la violencia contra las mujeres e integrantes del grupo familiar, conforme a la Ley 30364.

Como se puede verificar, en un inicio no se tenía muy en claro cuál sería la naturaleza del sistema de IA que involucraría a Amauta, pero sí se destacó que se buscaba que funcionara como un asistente jurisdiccional respecto de la elaboración de medidas de protección vinculadas con la aplicación de la Ley 30364.

Al año siguiente, el 5 de febrero de 2024, la Corte publicó la Resolución Administrativa 162-2024-P-CSJLIMANORTE-PJ, en cuyos considerandos tercero, cuarto y quinto se mencionó que para el desarrollo de Amauta:

- Se adquirieron Unidades de Procesamiento de Gráficos de alto rendimiento y se capacitó al personal encargado.
- Se dotó a dicho personal con ambientes con alta conectividad e interoperabilidad.
- Se lograron avances vinculados con la extracción de datos que ingresan mediante la interoperabilidad (pudiéndose convertir en texto editable), con el etiquetado de la información en campos específicos de los modelos de resoluciones estándar, entre otros, que llevaron a estructurar a Amauta como un SE para la emisión de resoluciones judiciales basadas en reglas ¹³.

¹² Resolución Administrativa 1086-2023-P-CSJLIMANORTE-PJ del 18 de agosto de 2023.

¹³ Resolución Administrativa 162-2024-P-CSJLIMANORTE-PJ del 5 de febrero de 2024. Resulta pertinente citar el considerando quinto: “Quinto: Los avances en la implementación y desarrollo del proyecto Amauta. Pro son alentadores: se ha logrado la extracción de datos de los documentos (pdf, imágenes y texto) que ingresan por interoperabilidad, a través del SIPROVIV (Sistema de Protección de

Esta es la primera resolución de la Corte en la que se hace referencia a que se estaba apuntando a que Amauta se constituyera un SE. Asimismo, algo importante a destacar es la referencia a la interoperabilidad, que es un concepto muy relevante en materia de Gobierno Digital, y que apunta a la posibilidad de permitir un intercambio de datos e información entre entidades públicas en este caso, con la finalidad de conseguir en tiempo real los insumos necesarios para la toma de decisiones, sirviendo como un elemento imprescindible para asegurar que los productos que ofrezca un SE como Amauta puedan ser los más provechosos posibles.

Cabe resaltar que respecto de la interoperabilidad de datos e información necesaria para el funcionamiento de Amauta sobre la base del funcionamiento de la Plataforma de Interoperabilidad del Estado (PIDE), podemos presumir que las entidades públicas involucradas serían las siguientes:

- La Policía Nacional del Perú (PNP), cuyos policías recaban los datos y la información de las denuncias presentadas en el marco de la Ley 30364, y que procesan las denuncias y reportes respectivos.
- El Programa Nacional para la Prevención y Erradicación de la Violencia contra las Mujeres e Integrantes del Grupo Familiar – Aurora, cuyos servidores civiles realizan labores similares a los de los policías respecto de los datos e información que recopilan.
- El Ministerio Público, cuyos Fiscales y personal de apoyo procesan las denuncias, los reportes y los informes que son puestos a su conocimiento por la Policía Nacional del Perú (PNP) y el Programa Aurora.

El 25 de abril de 2024, la Corte publicó la Resolución Administrativa 418-2024-P-CSJLIMANORTE-PJ, en cuyos considerandos sétimo y

Víctima de Violencia de la PNP); se ha logrado convertir dicha información en texto editable en una plantilla estandarizada para el Expediente Judicial Electrónico del Módulo de Violencia de la Corte de Lima Norte; se ha conseguido ordenar y etiquetar la información en campos específicos de los modelos de resoluciones estándar, en función de reglas aprobadas por los jueces de familia; se ha logrado identificar el tipo de violencia y el nivel de riesgo de la víctima; se ha procesado el texto que las describe y las medidas vinculadas, entre otros logros, que progresivamente están permitiendo estructurar un sistema experto de emisión de resoluciones judiciales basado en reglas”.

octavo se destacó que Amauta, como resultado del proceso de desarrollo y las etapas de pruebas, redefinió su concepto inicial, siendo considerado como un SE basado en reglas, programado con modelos y algoritmos de IA, que emite proyectos de resolución de manera automatizada, extrayendo información de los documentos electrónicos del Expediente Judicial Electrónico del Poder Judicial (EJE PJ) y la PIDE¹⁴.

Dicha resolución autoriza la etapa de pruebas y mejoras de Amauta, y considerando lo expuesto, es redefinido como un SE en los términos indicados para la elaboración de resoluciones de manera automatizada en el marco de la Ley 30364, Ley de Protección, Sanción y Erradicación de la Violencia Contra las Mujeres y los integrantes del grupo familiar.

Al tener mucho más claro a estas alturas que Amauta es considerado un SE, es muy importante verificar qué tipo de SE constituye debido a que existen varios tipos considerando sus características. Al respecto, Richard Susskind en otro de sus artículos los clasifica en cinco tipos¹⁵:

¹⁴ Resolución Administrativa 418-2024-P-CSJLIMANORTE-PJ del 25 de abril de 2024. Los considerandos indicados describen con mucho detalle el funcionamiento de Amauta en su calidad de SE: “**Sétimo.-** En el proceso de desarrollo y en las etapas de pruebas, el asistente virtual “Amauta.Pro” ha redefinido su concepto inicial, de modo que por su arquitectura y funcionalidad, ahora se puede definir como un asistente virtual basado en reglas, programado con modelos y algoritmos de inteligencia artificial que emite proyectos de resolución de manera automatizada en el marco de la Ley 30364, Ley de Protección, Sanción y Erradicación de la Violencia Contra las Mujeres y los integrantes del grupo familiar.

Octavo.- La funcionalidad de Amauta.Pro nos permite describirlo como un sistema experto basado en reglas que se conecta al almacén de documentos electrónicos del Expediente Judicial Electrónico (EJE) del Poder Judicial; lee el expediente remitido en formato PDF por la Policía Nacional del Perú y convierte la información en texto editable. Extrae, edita y mejora la redacción de los párrafos necesarios para crear los proyectos de resolución. De la misma forma, se conecta a la base de datos del EJE y a la Plataforma de Interoperabilidad del Estado (PIDE) para extraer los demás párrafos y datos que se integran en plantillas de resoluciones estandarizadas. Finalmente, estructura toda la información y genera el proyecto de resolución que concede medidas de protección para las mujeres y los integrantes del grupo familiar en riesgo de violencia”.

¹⁵ SUSSKIND, R. (1990). Artificial Intelligence, Expert Systems and Law. The Denning Law Journal, pp. 106-107.

- Sistemas diagnósticos: ofrecen soluciones específicas para problemas presentados ante ellos.
- Sistemas de planificación: ayudan a definir escenarios estratégicos para minimizar riesgos legales.
- Guías de procedimiento: brindan pautas concretas para resolver los problemas en el marco de un procedimiento legal.
- Lista de verificación inteligente: apoya a la verificación del cumplimiento de normas legales.
- Sistemas de modelación de documentos: generan documentos específicos sobre la base de su conocimiento de manera automática.

Con relación a Amauta, y en atención a lo desarrollado, parece que nos encontramos frente a un SE que se constituye en un sistema de modelación de documentos, debido a que, en atención a los conocimientos programados respecto de la normativa aplicable y los datos e información incluidos en el EJE PJ de los que se alimenta, complementado con los datos e información extraídos como resultado de la interoperabilidad con otras entidades públicas por medio de la PIDE, produce proyectos de resoluciones judiciales como apoyo a la labor de los jueces involucrados.

El 24 de setiembre de 2024, la Corte publicó la Resolución Administrativa 973-2024-P-CSJLIMANORTE-PJ del 24 de setiembre de 2024, en cuyo considerando cuarto se hizo referencia a que Amauta fue objeto de mejoras en sus funcionalidades y en su capacidad de procedimiento y transmisión de datos, habiendo asistido a los jueces en la emisión de proyectos de resolución en el marco del período de marcha blanca, por lo que correspondía oficializar el inicio de su producción¹⁶.

En línea con lo precisado, la mencionada resolución dispuso el inicio oficial del período de producción de Amauta, brindando apoyo a once juzgados vinculados con la aplicación de la Ley 30364, aprobando el uso de cinco plantillas referentes a las resoluciones que dictan medidas de protección para los casos de: 1) violencia de pareja, 2) adulto mayor, 3) niñas, niños y adolescentes, 4) incompetencia, 5) Inhibición.

¹⁶ Resolución Administrativa 973-2024-P-CSJLIMANORTE-PJ del 24 de setiembre de 2024.

Considerando que nos encontramos en los primeros meses de implementación de Amauta, que podemos considerar como un SE pionero en el Poder Judicial de Perú, es importante hacer referencia a las limitaciones que pueden presentar en general los SE, a fin de evitar que sus efectos perjudiciales sobre su funcionamiento se puedan presentar en su aplicación concreta.

Como parte de las limitaciones de los SE, podemos destacar que, al encontrarnos frente a su aplicación en el ámbito jurídico, se presentan situaciones que los distinguen de los SE que aparecen, por ejemplo, en el ámbito de la salud.

En efecto, en el caso de estos últimos, los SE tienen su base en las leyes de las ciencias naturales, las cuales se sustentan en la experiencia, siendo causales y descriptivas, lo que no se configura en el razonamiento legal, el cual involucra a la manipulación interpretativa de las normas prescriptivas del ordenamiento jurídico, las que no se plantean de manera uniforme o bajo patrones en el mundo exterior, sino que se desprenden del escrutinio de las fuentes formales de las normas¹⁷.

Esto implica que, si los SE se desempeñan de manera más precisa y exacta en el ámbito de la salud, ello se debe a que el conocimiento que les sirve de sustento y las reglas aplicables tienen un margen más acotado para el razonamiento que pueda desarrollarse, considerando que sus parámetros son más estables y se basan con más claridad en las experiencias previas.

La situación descrita no ocurre necesariamente en el caso del razonamiento jurídico aplicable en el marco de un proceso judicial, debido a que, si bien el contenido de las normas puede llegar a ser consistente en el tiempo, su interpretación es muy variable, dependiendo de las valoraciones

¹⁷ SUSSKIND, R. (1986), *Artificial Intelligence, Expert Systems and Law*. The Denning Law Journal, pp. 181-182. El citado autor indica: "It might seem intuitively obvious that this lack of success stems from the differences between the nature of legal reasoning and the nature of other enterprises such as diagnosing illnesses, mineral prospecting, and inferring chemical structures. The latter, we generally agree, are rooted, ultimately, in the empirically-based, causal, descriptive laws of the natural sciences, whereas legal reasoning involves the manipulation of the prescriptive laws of the legal order, discoverable, in the main, not from uniformities or patterns in the external world but through scrutiny of the formal sources of the law".

personales de los diversos operadores jurídicos que se ven involucrados en los casos concretos, lo que genera que en algunos casos los productos de un SE (en el caso de Amauta, proyectos de resoluciones judiciales) no puedan ser los más adecuados, lo que resalta la importancia de la constante supervisión humana (en este caso de los jueces) para verificar su calidad y pertinencia antes de tomar sus decisiones.

Respecto de los operadores jurídicos involucrados en los procesos judiciales vinculados con los proyectos de resoluciones a cargo de Amauta, podemos presumir que se encuentran vinculados con:

- Los policías que recaban los datos y la información de las denuncias presentadas en el marco de la Ley 30364, y que procesan las denuncias y reportes respectivos.
- Los servidores civiles del Programa Aurora, que realizan labores similares a los de los policías respecto de los datos e información que recopilan.
- Los Fiscales y su personal de apoyo que procesan las denuncias, los reportes y los informes que son puestos a su conocimiento por la PNP y el Programa Aurora.
- Los Jueces y su personal de apoyo que toman conocimiento de los datos e información incluidos en los documentos ofrecidos por la PNP, el Programa Aurora y las Fiscalías, así como del propio Poder Judicial mediante el EJE PJ.

Considerando la cantidad de operadores jurídicos involucrados, cada uno con funciones y responsabilidades distintas, se presenta un escenario en el que es importante tener presente la definición clara de criterios para la extracción y el procesamiento de los datos e información a ser recopilados y procesados por el SE, a fin de evitar que sus productos se vean distorsionados, evitando de esa manera obtenerse la utilidad esperada con su empleo.

Es clave tener esto en cuenta, debido a que en el caso de los SE es muy difícil llegar a obtener una contundencia a nivel jurisprudencial tomando en cuenta que su funcionamiento se puede ver afectado por quiénes los usan, la forma en que son usados, y las limitaciones que se presentan al intentar resolver problemas jurídicos teniendo en cuenta sólo algunas de las reglas que pueden ser aplicadas, sin poder abarcar un análisis más

amplio, como el que sería posible empleando, por ejemplo, principios jurídicos¹⁸.

No obstante lo expuesto, es importante reiterar que los SE pueden constituirse en un apoyo intelectual de alto nivel para la labor de los jueces, debiéndose tener en cuenta diversos aspectos para asegurar su éxito, tales como los siguientes¹⁹:

- Debe realizarse un estudio riguroso sobre la factibilidad de la implementación del SE en el ámbito jurídico, de manera previa a su desarrollo con mayor amplitud: En el caso de Amauta, se aprecia que el referido estudio se ha realizado, en atención a que desde el año 2023 se ha venido estudiando la aplicación del referido sistema de IA, habiéndose desarrollado un período de prueba de manera previa al inicio de su producción oficial para productos específicos.
- Es clave asegurar un período de prueba de los prototipos en una etapa temprana, para mejorar el entendimiento de la gestión, el conocimiento y los posibles usuarios del SE: Como se afirmó en el literal anterior, antes del lanzamiento de Amauta se efectuaron pruebas durante un período de marcha blanca.
- Las habilidades convencionales en el procesamiento de datos pueden y deben ser usados regularmente en el curso del desarrollo

¹⁸ *Ibid.*, pp. 111. El citado autor indica: “Jurisprudential soundness (...) there are no fundamental objections from the point of view of legal philosophy to building expert systems in law of limited scope. These limitations in scope refer to the category of proper user (the lawyer or legally informed person); the way in which such a system should be used (as an ‘intelligent assistant’ and not a replacement for a legal expert); and the limitations of solving problems on the basis only of legal rules (so that these systems currently cannot reason on the basis of legal principle, policy or purpose)”.

¹⁹ *Ibid.*, pp. 115-116. El citado autor indica: “A rigorous feasibility study must be undertaken prior to any major development project. Quick, inexpensive prototyping of systems can, at an early stage, greatly enhance the understanding of management, experts, and projected users. (...) Conventional data processing skills can and should be regularly used in the course of developing expert systems in law. A fundamental, theoretical, jurisprudential understanding of the law on the part of developers greatly increases the likelihood of the development of reliable systems. Once in operation, the performance and organisation fit of systems must frequently be monitored”).

de SE jurídicos: Esto es muy importante en el caso de Amauta, sobre todo considerando que la gestión de datos involucra al EJE PJ y a la interoperabilidad mediante la PIDE con varias entidades públicas.

- Una comprensión fundamental, teórica y jurisprudencial del Derecho por parte de los desarrolladores incrementa en gran medida la posibilidad del desarrollo de SE confiables: Un factor importante es que la base de conocimientos que nutra a Amauta se encuentre actualizada y sustentada, además de los datos e información que extrae y recopila, en un conocimiento experto en las materias involucradas, como el Derecho de Familia, Derecho Procesal, Derecho Penal, Derecho Administrativo, entre otros.
- Una vez en operación, el desempeño y la adecuación organizacional del SE deben ser monitoreados frecuentemente: Eso es algo que debe realizarse en el caso de Amauta, con la finalidad de determinar qué aspectos pueden seguir afinándose sobre la base de criterios de mejora continua.

Respecto de la mejora continua de los SE, conviene hacer mención a un artículo reciente en el que se destacó la importancia de los “árboles de decisión” (decision trees) para mejorar su desempeño, los cuales no sólo brindan aportes basados en el conocimiento con el cual se programan, sino que dan un paso más: considerando dicho conocimiento, proponen las reglas para plantear las opciones que se pueden tomar ante la consulta sobre un problema determinado²⁰ (o respecto de qué posible decisión reflejar en un proyecto de resolución judicial, en el caso de Amauta).

El artículo propone dos mejoras concretas que podrían ser evaluadas en el caso de Amauta de estimarse pertinente:

- El uso de “árboles de decisión” generados mediante algoritmos: Esto permitirá que, mediante el ensayo y el error al interactuar con un SE como Amauta, los usuarios (incluso los que no cuenten con un

²⁰ MATHESON, A. (2024). Applied Artificial Intelligence for Law: The Use of Expert Systems and Decision Trees in Legal Practice and the Potential of Artificial Neural Networks. *Legal Issues Journal*, pp. 5. El citado autor indica: “Decision trees (as far as decision science is concerned) can do slightly more than act as taxonomies of knowledge since they can contain the rules regarding which paths should be followed”.

alto nivel de conocimiento sobre las materias involucradas), puedan construir una clasificación de las opciones disponibles desde una muestra de los datos que componen la base de conocimiento del SE²¹.

- Reforzar el alcance de los “árboles de decisión” con los avances de la ciencia de decisiones: Con este refuerzo, las opciones disponibles no sólo reflejarán un curso de acción específico, sino que también brindarán insumos sobre cada una de dichas opciones, incluyendo los posibles resultados que se obtendrían al escogerlas²².

Tomando en cuenta las limitaciones de los SE y los criterios para garantizar el éxito y la mejora continua en su implementación, sistemas como Amauta podrán servir de mucho para mejorar la calidad y oportunidad de los productos, en este caso resoluciones judiciales, que emita el Poder Judicial de Perú, beneficiando de esa manera a los ciudadanos involucrados en los procesos judiciales.

V. Conclusiones

Los SE forman una parte del campo del conocimiento de la IA que se enfoca en la generación de insumos sobre una base de conocimientos y un motor de inferencia en el que los seres humanos tienen una participación activa y un nivel de control respecto de su funcionamiento.

Estas condiciones permiten que el funcionamiento del SE posea un nivel de transparencia adecuado que refleje cómo es que los productos que proporciona son obtenidos sobre la base de los datos y la información que extrae y que procesa, lo que permite comprender sus alcances

²¹ *Ibid.*, pp. 7. El citado autor indica: “Using algorithmically generated decision trees (...) Through automated trial, error and elimination, with no need for expertise, a system can be programmed to build a classification tree from a sample of data”.

²² *Ibid.*, pp. 8. El citado autor indica: “Borrowing from the domain of decision science (...) The decision trees of decision science are not simply navigation tools like those described above but are enriched with information to allow either decisions to be taken by a human operator with better information available at each step, or to allow a system to calculate an optimal route through a decision tree in the same way that a satellite navigation system not only displays a digital map but can calculate an optimal route through it. These are decision trees that not only contain structured information about a set of decisions but are also enriched with information about possible outcomes at each decisión junction”.

y limitaciones a la hora de constituirse en un insumo para la toma de decisiones judiciales.

Si bien lo anterior es una clara ventaja respecto de sistemas de IA más modernos que poseen un alto nivel de opacidad y permite que los SE puedan ajustarse a los criterios establecidos en documentos internacionales sobre la materia publicados en Reino Unido y Colombia, es importante no perder de vista que los SE poseen limitaciones que pueden afectar sus resultados, como los que se presentan al considerar que estamos frente a un apoyo respecto de una actividad tan compleja como lo es el razonamiento jurídico, el cual está sujeto a la diversa interpretación de todos los operadores jurídicos que intervienen en su funcionamiento, tal como lo vimos en el caso de Amauta.

Aunado a lo anterior, también es importante tomar en cuenta que el funcionamiento de un SE como Amauta depende mucho de una adecuada interoperabilidad entre las entidades públicas participantes en su base de conocimiento, siendo clave garantizar que la interacción entre ellas sea la más fluida posible.

Amauta se constituye en un SE pionero en el Poder Judicial de Perú, habiéndose constituido de manera reflexiva sobre la base de un diagnóstico previo y un período de prueba que permitió afinar su naturaleza y funcionamiento, cumpliendo con varias de las recomendaciones para el éxito de un SE.

Sin embargo, es clave no descuidar el inicio de la implementación de Amauta y mantener una supervisión constante de su funcionamiento sobre la base de su mejora continua, más aún si no se cuenta todavía con una normativa jurídica o lineamientos aplicables a su uso por parte del Poder Judicial de Perú, evaluando implementar las medidas correspondientes para que sus productos (resoluciones judiciales) sean cada vez de mayor utilidad para sus principales operadores jurídicos: los jueces, lo que redundará en una administración de justicia de mayor calidad en beneficio de los ciudadanos.

Justicia y algoritmos: Un análisis ético-jurídico de la Ley 31814 sobre inteligencia artificial en el Perú

Blanca Lizbeth Carrasco Delgado*

Resumen.- La inteligencia de inteligencia artificial en el sistema judicial plantea tensiones con principios constitucionales como el debido proceso, la motivación de las resoluciones y la garantía del juez natural. A partir de un enfoque ético-jurídico, se examina la Ley 31814, advirtiendo su insuficiencia normativa frente a los riesgos algorítmicos, y se proponen criterios para una regulación sustancialmente justa.

Palabras clave.- Inteligencia artificial – justicia algorítmica – sesgos – regulación jurídica – ética judicial.

Abstract.- The incorporation of artificial intelligence into the judicial system raises tensions with constitutional principles such as due process, the reasoning of decisions, and the guarantee of a natural judge. From an ethical-legal perspective, this article examines Law No. 31814, highlighting its normative insufficiencies in addressing algorithmic risks, and proposes criteria for a substantively just regulation.

Keywords.- Artificial intelligence – algorithmic justice – biases – legal regulation – judicial ethics.

* Coordinadora de la Unidad de Derecho de la Escuela de Posgrado Newman y docente de la misma casa de estudios. Se especializa en Derecho de la Empresa, compliance, nuevas tecnologías aplicadas al Derecho y arbitraje. Abogada con un MBA y actualmente cursa doctorado en Derecho, con estudios de posgrado en Finanzas, Marketing y Gestión Legal Corporativa.

I. Introducción

La inteligencia artificial (en adelante, “IA”) ha marcado un cambio significativo en diversos sectores, y la administración pública no ha quedado exenta de esta transformación. En particular, en el ámbito judicial, la implementación de la IA ha permitido optimizar procesos, mejorar la eficiencia y reducir los tiempos de resolución de casos. A través de algoritmos y sistemas automatizados, se busca agilizar las decisiones judiciales y facilitar el acceso a la justicia. No obstante, la adopción de estas tecnologías plantea interrogantes profundos sobre su capacidad para garantizar la equidad, la transparencia y el respeto a los derechos fundamentales. La delegación de decisiones judiciales a sistemas algorítmicos ha suscitado debates acerca de si estos pueden tomar decisiones que respeten principios esenciales como el debido proceso y la dignidad humana. La opacidad de los algoritmos, el riesgo de sesgos en los datos utilizados y la ausencia de empatía en las decisiones automatizadas generan preocupaciones sobre la posible vulneración de derechos fundamentales, lo que pone en duda la idoneidad de la IA en cuestiones tan delicadas como las decisiones judiciales. Ante este panorama, el objetivo de este artículo es analizar el alcance de la potestad reguladora del Estado frente a la IA judicial, en el contexto de la Ley 31814 del Perú y otras experiencias internacionales, abordando el tema desde una perspectiva jurídico-ética. A través de este análisis, se busca explorar cómo el Estado puede regular el uso de la IA en la administración de justicia, asegurando que su implementación sea ética y respetuosa de los derechos fundamentales de las personas.

II. Marco legal peruano

i. Fundamentos constitucionales

La Constitución Política del Perú, en su artículo 139, consagra un conjunto de principios esenciales que rigen la función jurisdiccional y que resultan especialmente relevantes ante el avance de tecnologías como la inteligencia artificial (IA) en el ámbito judicial. El debido proceso, la motivación de las resoluciones judiciales y la garantía del juez natural no solo constituyen reglas formales de procedimiento, sino que, conforme al desarrollo doctrinal y jurisprudencial, configuran auténticos derechos fundamentales que estructuran el sistema de justicia.

Desde una lectura constitucional garantista, el principio del debido proceso (art. 139.3) implica la obligación del Estado de asegurar a todas las personas el acceso a un proceso imparcial, con garantías mínimas que permitan ejercer el derecho de defensa, la contradicción probatoria y la obtención de una resolución dentro de un plazo razonable¹.

Uno de los elementos esenciales de este principio es la motivación de las resoluciones judiciales, recogida en el inciso 5 del mismo artículo constitucional, la cual constituye una garantía de racionalidad, transparencia y control. La motivación permite comprender las razones de una decisión, facilita su impugnación y asegura que los jueces no actúen de manera arbitraria². En el contexto del uso de IA, esta exigencia se complejiza, ya que los sistemas algorítmicos no siempre permiten una trazabilidad clara de sus procesos de decisión, lo que podría generar serias tensiones con esta exigencia constitucional, especialmente cuando se trata de modelos de aprendizaje automático con lógica opaca o cajas negras³.

Por otro lado, el derecho al juez natural (art. 139.1 y 139.2) garantiza que toda persona sea juzgada por una autoridad previamente establecida por ley, independiente, imparcial y competente. Este principio, además de proteger frente a la arbitrariedad del Estado, sostiene el carácter humano del acto de juzgar⁴, lo cual se torna particularmente relevante frente a los procesos de automatización jurisdiccional. La doctrina iusfilosófica, en especial la inspirada en el pensamiento de Javier Hervada, advierte que el acto de juzgar no puede ser reducido a la aplicación mecánica de reglas, ya que implica prudencia, contexto y equidad⁵. Así, frente al avance de modelos de justicia algorítmica, se debe salvaguardar la intervención

¹ LINARES, S. (2023). Garantías procesales frente a decisiones automatizadas: el debido proceso ante la inteligencia artificial. *Revista Iberoamericana de Derecho Procesal*, 17(1), pp. 45-66.

² LÓPEZ, M. (2018). Motivación judicial y transparencia en el debido proceso. *Revista Peruana de Derecho Constitucional*, 9(1), pp. 45-68.

³ GONZÁLEZ, M. (2022). Motivación de las decisiones automatizadas y transparencia algorítmica en el proceso judicial. *Revista Española de Derecho Constitucional*, (124), pp. 221-245.

⁴ MUÑOZ, R. (2024). El principio del juez natural ante los sistemas de justicia automatizada. *Estudios Constitucionales*, 22(1), pp. 133-158.

⁵ SANTA CRUZ, J. (2024). Racionalidad limitada y sesgos cognitivos judiciales. *Revista Oficial del Poder Judicial*, 16(22), pp.225-261.

activa de jueces humanos como garantía de justicia sustancial y no meramente formal.

Desde la doctrina nacional, autores como Tupayachi⁶ y Santa Cruz⁷ han alertado sobre los riesgos que la IA representa frente a estos principios. En particular, se advierte que el uso de sistemas automatizados en procedimientos constitucionales de tutela puede debilitar la garantía del debido proceso si no se establecen mecanismos efectivos de supervisión humana y explicabilidad algorítmica. En la misma línea, Ávila Paz de Robledo⁸ sostiene que una implementación legítima de la IA judicial requiere el cumplimiento de criterios mínimos como la trazabilidad, la transparencia, la supervisión humana constante y una estructura normativa que permita la rendición de cuentas. Estos elementos no solo son exigencias técnicas, sino que encuentran respaldo constitucional en los principios del artículo 139, que deben guiar toda innovación dentro del sistema de justicia.

En síntesis, el marco constitucional peruano establece un estándar normativo robusto que impone condiciones materiales para la incorporación de tecnologías como la inteligencia artificial en el ámbito judicial. Cualquier intento de automatización en este sector deberá respetar, sin excepción, el debido proceso, la motivación de las decisiones y la garantía del juez natural, principios que no pueden ser relativizados por razones de eficiencia técnica. El desafío ético-jurídico no radica en rechazar la tecnología, sino en adaptarla al servicio de la justicia sin sacrificar las garantías fundamentales que sostienen el Estado de derecho.

ii. La Ley 31814

Una vez establecidos los límites constitucionales al uso de la IA en la justicia, corresponde ahora analizar la Ley N.º 31814, norma marco que intenta regular el desarrollo y uso responsable de esta tecnología en el país.

⁶ TUPAYACHI, J. (2024). La aplicación de la inteligencia artificial en los procesos constitucionales de tutela de derechos fundamentales. *Revista Oficial del Poder Judicial*, 16(22), pp. 99-125.

⁷ SANTA CRUZ, J. (2024). Racionalidad limitada y sesgos cognitivos judiciales. *Revista Oficial del Poder Judicial*, 16(22), pp. 225-261.

⁸ ÁVILA, R. (2023). Proceso judicial digital e inteligencia artificial: nuevos horizontes. *Anuario CIJS, UNC*.

La Ley 31814⁹ fue promulgada en el Perú con el objeto de establecer principios orientadores para el uso de la inteligencia artificial (IA) como herramienta para el desarrollo económico y social del país. Si bien esta norma representa un avance en términos de reconocimiento estatal del fenómeno tecnológico, su alcance real y su capacidad regulatoria efectiva han sido objeto de críticas desde diversos sectores académicos y técnicos. En términos generales, se trata de una ley programática, con efectos esencialmente declarativos, y con escasa operatividad normativa en ámbitos específicos como el judicial.

Esta ley establece un marco normativo orientado al uso ético y responsable de la IA en el país. Aunque su alcance es amplio, abarcando sectores como la salud, educación, agricultura y seguridad, su aplicación en el ámbito judicial es aún incipiente. La ley destaca principios rectores como la ética, la transparencia y la no discriminación, y establece la obligación del Estado de fomentar un desarrollo responsable de la IA. Sin embargo, carece de regulaciones específicas que guíen su implementación en el sistema judicial, lo que limita su aplicabilidad en este sector. El carácter no vinculante de la ley, aunque orientador para políticas públicas, no impone obligaciones legales directas, lo que podría contribuir a la falta de avances en la integración de la IA en la administración de justicia¹⁰.

El artículo 1 de la ley señala que su objeto es promover el uso de la inteligencia artificial “en el marco del proceso nacional de transformación digital”, privilegiando el respeto de los derechos humanos y la ética. Sin embargo, el texto no contiene disposiciones que impongan obligaciones jurídicas específicas a los poderes del Estado ni al sector privado. De hecho, no existe una mención directa al Poder Judicial, ni se regulan expresamente los usos de IA en procesos jurisdiccionales, lo que implica que su aplicación al ámbito judicial es meramente indirecta y sujeta a interpretaciones abiertas.

⁹ Ley 31814. (2023). Ley que promueve el uso de la inteligencia artificial en favor del desarrollo económico y social del país. *Diario Oficial El Peruano*, 5 de julio de 2023.

¹⁰ MEDINA, Á., ORTIZ, M., & OROZCO, D. (2025). Pasado, presente y Futuro de la Inteligencia Artificial en la Salud: Entre Innovación y Seguridad. *Actualidad Jurídica Iberoamericana*, (22), pp. 942-969.

La literatura académica coincide en que esta norma carece de los elementos estructurales que caracterizan a una regulación tecnológica robusta. Reyna López, Milián Requena y Romero Vélez¹¹ destacan que la Ley N.º 31814 no contempla una clasificación por niveles de riesgo como lo hacen otros marcos comparados. En su análisis comparativo con el AI Act europeo, señalan que mientras este último distingue entre usos de riesgo inaceptable, alto, limitado y mínimo, la legislación peruana no introduce ninguna tipología similar ni prevé evaluaciones de impacto.

Asimismo, se observa la ausencia de mecanismos de trazabilidad y explicabilidad algorítmica. La ley no exige que los sistemas de IA puedan justificar sus decisiones ni provee garantías sobre su comprensibilidad por los usuarios o afectados, lo cual compromete seriamente la posibilidad de cumplir con principios constitucionales como la motivación de las resoluciones judiciales. Tampoco se establecen protocolos de supervisión humana significativa, una exigencia reiterada por organismos internacionales como UNESCO o el Consejo de Europa.

La Recomendación de la UNESCO establece un marco ético y normativo para la IA, enfocándose en la protección de los derechos humanos y la dignidad humana. En el contexto judicial, se hace hincapié en la necesidad de principios como la equidad, la transparencia, y la responsabilidad en el uso de la IA, para garantizar que los procesos judiciales sean justos y sin sesgos algorítmicos¹².

Además, se resalta la importancia de integrar estas normas en las legislaciones nacionales, promoviendo la confianza pública en la tecnología y evitando su abuso. El objetivo es asegurar que la IA se utilice de manera ética, respetando siempre los derechos fundamentales de las personas.

Flor Flores¹³ advierte que este vacío es especialmente preocupante en el contexto de justicia algorítmica, pues una normativa que no exige

¹¹ REYNA, G., MILIÁN, C., & ROMERO, X. (2025). Inteligencia artificial y derecho informático, retos y oportunidades para las legislaciones actuales. *IGOVERNANZA*, 8(29), pp. 109-126.

¹² BRAVO-PLACERES, I. (2025). Entre algoritmos y justicia: la danza regulatoria de la inteligencia artificial. *IUSTITIA SOCIALIS*, 10(18), pp. 5-25.

¹³ FLOR, A. (2024). La vulneración de los derechos fundamentales a través de la inteligencia artificial. *Sapientia & Iustitia*, (11), pp. 5-24.

trazabilidad ni auditabilidad puede facilitar escenarios de discriminación o vulneración de derechos sin responsabilidad institucional clara. En este sentido, la autora concluye que la ley se limita a enunciar principios éticamente deseables, pero carece de mecanismos de aplicación, fiscalización o sanción que los vuelvan exigibles. La supervisión humana, cuando es mencionada, aparece como una expectativa política general, no como un estándar técnico-normativo operativo.

Apesar de que el artículo 4 de la norma designa a la Secretaría de Gobierno y Transformación Digital como la autoridad nacional competente, su función se limita a la promoción de políticas, sin facultades regulatorias ni coercitivas. A la fecha de elaboración de este artículo, el reglamento prometido por la Disposición Complementaria Final aún no ha sido publicado, lo que impide delimitar claramente las competencias y mecanismos para el cumplimiento de la ley.

En conclusión, si bien la Ley N.º 31814 constituye un esfuerzo pionero por incorporar el tema de la inteligencia artificial en la agenda legislativa peruana, su diseño normativo es insuficiente para afrontar los desafíos jurídicos que plantea la integración de IA en sectores sensibles como la administración de justicia. Al no establecer mecanismos de control, supervisión, corrección de sesgos ni evaluación de impacto, la ley no garantiza la compatibilidad del uso de IA con los principios constitucionales del debido proceso, la motivación de resoluciones y la tutela jurisdiccional efectiva. En este sentido, su impacto jurídico es aún marginal, y su efecto real depende de desarrollos normativos futuros que definan estándares vinculantes y adaptados a las particularidades del sistema judicial peruano.

iii. Análisis Ético de la Norma

A. Fundamentos ético-jurídicos para una justicia algorítmica humanista

El análisis ético del uso de inteligencia artificial en la justicia no puede reducirse a criterios técnicos de eficiencia, transparencia o auditabilidad. Estos elementos, si bien importantes, no bastan para garantizar una justicia sustancial. El presente trabajo asume una concepción ética desde el iusnaturalismo clásico, en la que la justicia es concebida como una virtud —no solo como adecuación a la norma positiva— y, por tanto, debe ser ejercida en clave de equidad, prudencia y respeto por la dignidad de la persona

humana¹⁴. Esta perspectiva permite evaluar no solo lo que es legal, sino lo que es legítimo y éticamente justo.

En este marco, la aplicación de algoritmos en decisiones judiciales plantea un dilema fundamental: ¿puede delegarse el juicio humano prudencial a una tecnología incapaz de valorar lo singular? Para autores como Ferrajoli¹⁵, el acto de juzgar requiere de motivación racional, ponderación de circunstancias y comprensión del contexto humano, elementos que son incompatibles con procesos de decisión automatizados basados en modelos estadísticos. Desde esta visión, la ética jurídica no se limita a respetar procedimientos, sino a garantizar que las decisiones estén orientadas al bien común, preservando la autonomía, la singularidad y la racionalidad práctica del juez.

Zorrilla¹⁶ sostiene que una ética pública de la inteligencia artificial debe responder a exigencias de justicia epistémica, participación, explicabilidad y control democrático. Ello exige que cualquier intervención de IA en procesos jurídicos esté sujeta a mecanismos efectivos de rendición de cuentas y al escrutinio público, evitando que las decisiones se tornen opacas o inapelables. La ética, por tanto, no puede concebirse como un valor abstracto o decorativo, sino como un principio ordenador del derecho y como límite sustantivo frente a la automatización acrítica del juicio.

La Ley N.º 31814 alude al “desarrollo ético” de la inteligencia artificial (art. único, e), pero no define qué se entiende por ello ni qué criterios sustantivos deberían observarse. Esta omisión diluye el contenido normativo del principio ético, reduciéndolo a una aspiración genérica y desprovista de exigibilidad. En contextos de justicia algorítmica, tal ambigüedad resulta particularmente peligrosa, pues puede abrir la puerta a decisiones automatizadas sin garantías adecuadas de equidad ni respeto por la dignidad del justiciable.

¹⁴ POLO, L. (2006). *Ética: Hacia una versión moderna de los temas clásicos*. Eunsa.

¹⁵ FERRAJOLI, L. (2011). *Derecho y razón: teoría del garantismo penal* (9.ª ed.). Trotta.

¹⁶ ZORRILLA, M. (2023). Inteligencia artificial y derechos humanos: bases para una ética pública en contextos de automatización. *Dilemata*, (42), pp. 89–110.

B. Riesgos éticos detectados en la Ley peruana

Una revisión crítica de la Ley N.º 31814 a la luz del marco ético propuesto permite identificar una serie de riesgos y vacíos regulatorios que comprometen su legitimidad desde la perspectiva del derecho natural y de los principios constitucionales fundamentales.

En primer lugar, el fenómeno de la “caja negra algorítmica” es completamente ignorado por la norma. No se contempla la necesidad de explicar cómo y por qué un sistema de IA toma determinadas decisiones, lo que impide garantizar la motivación exigida por el artículo 139 de la Constitución. Esta opacidad vulnera el principio de publicidad y razonabilidad de las decisiones judiciales, afectando la posibilidad de impugnarlas racionalmente¹⁷.

En segundo lugar, no se establece garantía alguna de supervisión humana significativa. La ley no exige que las decisiones automatizadas sean revisadas o validadas por operadores jurídicos humanos. Esto resulta incompatible con el carácter personal, prudencial e irrepetible del acto de juzgar, tal como ha sido desarrollado desde el pensamiento iusnaturalista¹⁸ y reiterado en estándares internacionales como los de la Unión Europea¹⁹.

Tercero, la ley omite por completo una regulación judicial específica. A pesar de mencionar al sector justicia entre los ámbitos donde se promoverá el uso de IA, no se incluyen criterios normativos diferenciados, ni se toma en cuenta la naturaleza cualitativamente distinta que supone intervenir con algoritmos en procesos que afectan derechos fundamentales.

Por último, la Ley N.º 31814 no contempla mecanismos para la detección y corrección de sesgos algorítmicos. Tampoco incorpora directrices para la evaluación de impacto en derechos ni estándares de no discriminación algorítmica. Esta ausencia resulta crítica, considerando la evidencia internacional que demuestra cómo los

¹⁷ FLOR, A. (2024). La vulneración de los derechos fundamentales a través de la inteligencia artificial. *Sapientia & Iustitia*, (11), 5–24.

¹⁸ HERVADA, J. (1991). *Introducción crítica al Derecho Natural* (3.ª ed.). Eunsa.

¹⁹ LEON, C. (2023). La carrera por la regulación de la inteligencia artificial. *Revista Latinoamericana de Economía y Sociedad Digital*, pp. 1-21.

modelos de IA pueden replicar y amplificar patrones estructurales de exclusión o injusticia²⁰.

Desde la perspectiva de la ética jurídica, estos vacíos no son solo problemas técnicos, sino fallas estructurales que cuestionan la legitimidad de la norma. Una ley que pretende orientar el uso de IA en sectores estratégicos del Estado debe incorporar criterios materiales de justicia, garantizar la protección de los derechos fundamentales y asegurar mecanismos efectivos de control, rendición de cuentas y corrección de errores.

Estos déficits evidencian una debilidad normativa estructural. Para contrastar esta situación, resulta pertinente revisar las experiencias regulatorias de otras jurisdicciones que ya han avanzado en el diseño de marcos ético-jurídicos sobre IA.

iv. Comparación Internacional

A. Principios y marcos normativos internacionales sobre IA judicial

Diversas instituciones, como la OCDE, UNESCO y el Consejo de Europa, han propuesto principios éticos orientadores en IA judicial, tales como explicabilidad, equidad, rendición de cuentas y seguridad algorítmica. El análisis comparado de marcos regulatorios sobre inteligencia artificial permite identificar buenas prácticas y deficiencias que sirven como referencia crítica para evaluar los alcances reales de la Ley N.º 31814 en el contexto peruano. Si bien cada sistema jurídico responde a condiciones normativas y sociales particulares, existe un consenso internacional emergente en torno a principios mínimos que deben regir el uso de IA en sectores sensibles como la administración de justicia. Estos principios incluyen la transparencia algorítmica, la trazabilidad de los sistemas, la supervisión humana significativa y la evaluación ex ante de riesgos para los derechos fundamentales.

Uno de los modelos más avanzados es el Reglamento de Inteligencia Artificial de la Unión Europea (AI Act), adoptado formalmente en 2024. Este cuerpo normativo clasifica los sistemas de IA según su

²⁰ REYNA, G., MILIÁN, C., & ROMERO, X. (2025). Inteligencia artificial y derecho informático, retos y oportunidades para las legislaciones actuales. *IGOBERNANZA*, 8(29), pp. 109-126.

nivel de riesgo (inadmisible, alto, limitado y mínimo), estableciendo obligaciones proporcionales a cada categoría. Los sistemas utilizados en la justicia están categorizados como de “alto riesgo”, por lo que están sujetos a requisitos estrictos, tales como la implementación de mecanismos de supervisión humana efectiva, la elaboración de documentación técnica detallada, el mantenimiento de registros de uso, la obligación de brindar información comprensible a los usuarios y la realización de evaluaciones de impacto en derechos fundamentales antes de su implementación efectiva²¹. Asimismo, el AI Act prohíbe expresamente el uso de sistemas de IA que impliquen manipulación subliminal, mecanismos de puntuación social y decisiones automatizadas sin posibilidad de revisión humana, en la medida que comprometan la autonomía, dignidad o privacidad de las personas²².

Otro referente normativo destacable es el modelo canadiense. La Directiva sobre la toma de decisiones automatizadas (Directive on Automated Decision-Making), emitida en 2020 por el Gobierno Federal, exige a todas las agencias públicas que realicen una evaluación de impacto algorítmico (Algorithmic Impact Assessment, AIA) antes de poner en funcionamiento un sistema de IA en procedimientos administrativos o jurisdiccionales. Esta herramienta permite identificar los posibles niveles de riesgo, analizar la existencia de sesgos discriminatorios, prever mecanismos de supervisión humana y diseñar canales adecuados para la apelación o revisión de decisiones automatizadas²³. Esta directiva también establece medidas de mitigación frente a impactos éticos y dispone la publicación obligatoria del análisis para garantizar la transparencia hacia los ciudadanos.

²¹ Parlamento Europeo y Consejo de la Unión Europea. Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo de 13 de junio de 2024 sobre normas armonizadas en materia de inteligencia artificial (Ley de IA). Diario Oficial de la Unión Europea, L 2024/1689.

²² *Ibid.*, artículos 5 y 6.

²³ Government of Canada. *Directive on Automated Decision-Making*. Treasury Board Secretariat, última modificación: 1 de abril de 2023. Obtenido de: <https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/responsible-use-ai/algorithmic-impact-assessment.html>

En suma, tanto el AI Act europeo como la Directiva canadiense expresan un cambio de paradigma hacia una gobernanza algorítmica basada en principios ético-jurídicos sustantivos. La experiencia comparada demuestra que, en contextos institucionales sólidos, la incorporación de inteligencia artificial en el sistema de justicia exige no solo normas programáticas, sino también obligaciones concretas, mecanismos de rendición de cuentas y dispositivos institucionales que garanticen que los sistemas algorítmicos estén al servicio de la justicia y no por encima de ella.

B. Experiencias concretas de uso de IA en sistemas judiciales comparados

Además de los marcos normativos, es pertinente examinar cómo se están aplicando en la práctica los sistemas de IA judicial en distintas jurisdicciones.

Uno de los casos más controvertidos en el uso de IA en justicia penal es el sistema *Correctional Offender Management Profiling for Alternative Sanctions* (COMPAS), ampliamente implementado en Estados Unidos para predecir la probabilidad de reincidencia delictiva. Diversas investigaciones han demostrado que este software presenta sesgos raciales sistemáticos: tiende a clasificar erróneamente a acusados afroamericanos como de alto riesgo, incluso sin antecedentes relevantes, mientras que los acusados blancos reciben con mayor frecuencia calificaciones de bajo riesgo. Estos sesgos reflejan desigualdades estructurales en los datos utilizados para entrenar el algoritmo, lo que genera graves consecuencias en la equidad del sistema judicial. Este ejemplo subraya la urgencia de incorporar mecanismos de corrección y supervisión en el diseño e implementación de sistemas algorítmicos, en línea con los principios de justicia sustantiva, soberanía digital y derechos humanos²⁴.

En Europa, Estonia ha desarrollado un modelo semiautomatizado para la resolución de reclamaciones de baja cuantía. En este sistema, los algoritmos generan órdenes de pago bajo control humano, lo

²⁴ IQBAL, R., & ISMAIL, S. (2025). Unbiased AI for a Sovereign Digital Future: A Bias Detection Framework. *Procedia Computer Science*, (254), pp. 118-126.

que permite resolver con rapidez disputas civiles menores. Desde 2019, se ha utilizado una IA especializada para resolver litigios inferiores a los €7,000, con el objetivo de mejorar la eficiencia sin comprometer las garantías procesales²⁵.

China, por su parte, ha implementado tribunales inteligentes que integran IA como el sistema “Xiaozhi”, diseñado para asistir a jueces en causas civiles mediante la recopilación automatizada de pruebas y la formulación de preguntas pertinentes. Si bien estas herramientas han optimizado algunos aspectos procesales, también han despertado críticas sobre su impacto en la independencia judicial, la transparencia y la capacidad de control humano²⁶.

Asimismo, en varias jurisdicciones europeas se están utilizando herramientas de jurisprudencia predictiva, las cuales emplean IA para estimar los resultados probables de casos judiciales. Estas tecnologías, sin embargo, presentan limitaciones importantes, especialmente en su capacidad para adaptarse a contextos sociales cambiantes. Por ello, el desarrollo regulatorio en Europa sigue en marcha, buscando garantizar condiciones mínimas de explicabilidad y equidad²⁷.

En América Latina, Brasil destaca como uno de los países más avanzados en esta materia. El proyecto de Ley Marco de IA, actualmente en debate parlamentario, propone la creación de una Autoridad Nacional de Inteligencia Artificial que supervise el uso ético de sistemas algorítmicos en el sector público. Además, reconoce el derecho de los ciudadanos a conocer los criterios que sustentan decisiones automatizadas, fortaleciendo así el principio de transparencia y control democrático²⁸.

²⁵ PARK, J. (2020). Your Honor, AI. *Harvard International Review*. <https://hir.harvard.edu/your-honor-ai/>.

²⁶ WANG, N., & TIAN, M. (2022). ‘Intelligent Justice’: AI Implementations in China’s Legal Systems. En K. Richardson & T. Heffernan (Eds.), *Social and cultural studies of robots and AI*, pp. 197-222. Springer.

²⁷ MEDVEDEVA, M., VOLS, M., & WIELING, M. (2019). Using machine learning to predict decisions of the European Court of Human Rights. *Artificial Intelligence and Law*, 28(2), pp. 237-266.

²⁸ SILVA, J. & NOBRE, M. (2023). Inteligência artificial e regulação: Perspectivas brasileiras e desafios globais. *Revista Brasileira de Direito Público*, 20(78), pp. 45–67.

Otros experimentos, como el caso de Kleros en arbitraje digital descentralizado, han demostrado que la ausencia de regulación específica puede generar serias incertidumbres jurídicas. En contextos como el peruano, esta falta de marco normativo plantea interrogantes sobre la validez, ejecutabilidad y legitimidad de decisiones tomadas parcial o totalmente por algoritmos²⁹.

Estas experiencias internacionales demuestran que, sin estándares éticos y jurídicos claros —como la trazabilidad, la revisión humana y la evaluación de riesgos—, toda regulación resulta insuficiente para enfrentar los desafíos que plantea la inteligencia artificial en el ámbito judicial. Por ello, el ordenamiento peruano debe incorporar urgentemente estos principios mínimos si aspira a una justicia realmente compatible con el Estado de Derecho.

Frente a estas experiencias, los vacíos de la Ley N.º 31814 se evidencian con mayor claridad. A diferencia de los marcos analizados, la legislación peruana no contempla una clasificación de riesgos, carece de exigencias sobre supervisión humana efectiva, no prevé evaluaciones de impacto previas ni establece estándares claros de trazabilidad. Además, no incorpora medidas sancionatorias frente al uso indebido de tecnologías algorítmicas.

En consecuencia, el Perú se encuentra rezagado frente a jurisdicciones que han optado por marcos regulatorios más exigentes y coherentes con el respeto a los derechos fundamentales. Las lecciones comparadas no exigen replicar modelos extranjeros, sino asumir estándares mínimos —precaución, explicabilidad, revisión humana y control democrático— que resultan imprescindibles para asegurar una justicia compatible con los principios del Estado de Derecho.

²⁹ CARRASCO, B. (2025). Blockchain y arbitraje digital en el Perú: ¿estamos listos para reconocer laudos descentralizados? *Anales de la Universidad Notarial Argentina*, (2), pp. 1-19.

III. Discusión y Propuestas

Las limitaciones advertidas tanto en el marco nacional como en los contrastes internacionales plantean la necesidad de proponer criterios concretos que orienten una regulación sustancialmente justa de la IA en el ámbito judicial.

La revisión crítica de la Ley N.º 31814, desde una perspectiva ético-jurídica centrada en la justicia sustancial, evidencia una preocupante disociación entre el discurso político de la transformación digital y la ausencia de garantías normativas mínimas para proteger los derechos fundamentales en contextos sensibles como la justicia. Si bien el reconocimiento de la inteligencia artificial como instrumento de desarrollo puede valorarse como una señal normativa positiva, ello no basta para justificar la omisión de mecanismos concretos de control y rendición de cuentas frente al uso de tecnologías potencialmente disruptivas.

La primera omisión estructural de la ley es la ausencia de una regulación específica para el ámbito judicial. Aunque el artículo 2 menciona al sistema de justicia como uno de los sectores en los que se promoverá el uso de IA, no se establece un régimen normativo diferenciado ni se contemplan criterios éticos o jurídicos específicos para el uso de algoritmos en decisiones jurisdiccionales. Esta omisión es grave, considerando que, como señala Hervada³⁰: “el acto de juzgar es un acto de equidad, de prudencia, de discernimiento contextual, imposible de reducir a una operación mecánica o estadística”.

La segunda carencia es la omisión del principio de subsidiariedad tecnológica, que debería consagrar que la inteligencia artificial solo puede operar como herramienta auxiliar del juez, y nunca como su reemplazo. Este principio ha sido reconocido en marcos normativos como el AI Act de la Unión Europea, que establece que los sistemas de alto riesgo, como aquellos aplicables en el poder judicial, deben estar sujetos a “supervisión humana significativa” y no pueden sustituir la deliberación jurídica prudencial³¹.

³⁰ HERVADA, J. (1991). *Introducción crítica al Derecho Natural* (3.ª ed.). Pamplona: Eunsu, p. 74.

³¹ LEON, C. (2023). La carrera por la regulación de la inteligencia artificial. *Revista Latinoamericana de Economía y Sociedad Digital*, pp. 1-21.

Además, se advierte la falta de mecanismos de explicabilidad, trazabilidad y evaluación de impacto ético-jurídico. Según Zorrilla³² “la justicia algorítmica requiere que toda decisión automatizada pueda ser reconstruida en su lógica, evaluada por agentes humanos competentes y sometida a control democrático” (p. 95). La ausencia de estos mecanismos en la Ley N.º 31814 compromete no solo el principio de motivación de las resoluciones judiciales, sino también el derecho de defensa y la posibilidad de interponer recursos con base en una comprensión razonada de la decisión.

Estos problemas no son únicamente fallas de técnica legislativa, sino que reflejan carencias profundas desde una visión de justicia sustantiva. En efecto, como ha señalado Luigi Ferrajoli, la existencia de normas legales sin mecanismos efectivos de control y garantía conduce a una legalidad puramente formal, incapaz de proteger derechos frente al poder estatal³³.

Frente a estos problemas, se proponen los siguientes lineamientos normativos esenciales, que podrían incorporarse en un futuro reglamento o en una ley especializada sobre IA judicial:

- Creación de un capítulo específico sobre IA judicial, con criterios de uso, limitaciones y condiciones para su implementación.
- Inclusión de requisitos técnicos obligatorios, como trazabilidad, explicabilidad, evaluaciones de impacto y protocolos de rendición de cuentas.
- Reconocimiento del principio de subsidiariedad tecnológica, garantizando que la decisión final recaiga en una autoridad judicial humana.
- Supervisión y auditoría independiente de los algoritmos, a cargo de un ente autónomo vinculado al sistema de justicia.
- Garantía del derecho a impugnar decisiones automatizadas, junto con la obligación estatal de asegurar vías de revisión humana integral.

³² ZORRILLA, M. (2023). Inteligencia artificial y derechos humanos: bases para una ética pública en contextos de automatización. *Dilemata*, (42), pp. 89–110.

³³ FERRAJOLI, L. (2022). *Poderes salvajes: la crisis de la democracia constitucional*, Madrid: Trotta, p. 46.

- Integración de una perspectiva de justicia sustancial, basada en la equidad contextual, la prudencia jurídica y la centralidad de la persona como límite infranqueable.

Estas propuestas buscan contribuir a una arquitectura regulatoria que armonice el uso legítimo de la IA con los fines superiores del derecho: proteger la dignidad humana, garantizar la racionalidad práctica del juzgador y asegurar que la justicia no se convierta en un resultado técnico, sino en un acto ético.

Además, la IA puede asistir en la toma de decisiones, pero nunca sustituir el discernimiento en derechos fundamentales. Investigaciones en el ámbito de la enfermería destacan que, aunque la IA mejora la eficiencia y personalización del cuidado, también puede deshumanizar el proceso si se prioriza la tecnología sobre la interacción humana³⁴. Por ello, la IA debe ser una herramienta al servicio de la humanidad, sin reemplazar el juicio ético y la dignidad inherente a cada persona.

IV. Conclusiones

El análisis ético-jurídico de la Ley N.º 31814 evidencia que su formulación, aunque representa un primer paso hacia la incorporación de tecnologías emergentes en el Estado peruano, resulta claramente insuficiente para regular de manera adecuada el uso de inteligencia artificial en el ámbito judicial. Si bien promueve principios como la ética, la transparencia y el desarrollo inclusivo, estos aparecen desprovistos de mecanismos normativos específicos que garanticen su aplicación efectiva, particularmente en sectores donde están en juego derechos fundamentales.

Desde una perspectiva de justicia sustancial, entendida como virtud y como realización del bien común, se constata que la norma adolece de criterios básicos como la supervisión humana significativa, la trazabilidad de decisiones automatizadas, la evaluación de impacto ético-jurídico y la obligación de explicabilidad de los algoritmos. Estas omisiones no son simplemente técnicas, sino estructurales, pues comprometen principios constitucionales como el debido proceso, la motivación de

³⁴ CASTRILLÓN, K., GIRALDO, J., & GARCIA, J. (2025). Riesgos y oportunidades de la inteligencia artificial en el cuidado de enfermería: una revisión de alcance. *Trilogía Ciencia Tecnología Sociedad*, 17 (35), pp. 1-29.

las resoluciones judiciales y la garantía del juez natural (Constitución Política del Perú, art. 139).

En línea con la doctrina iusnaturalista, debe afirmarse que la justicia no puede ser sustituida por la eficacia técnica. Como señala Hervada (1991), “la justicia es un acto prudencial, no mecánico; es razón práctica, no cálculo; es respeto por la dignidad del otro, no resolución de una función matemática” (p. 62). La ley, en su redacción actual, no asegura que estas condiciones se respeten en el uso de IA dentro del sistema judicial.

Asimismo, al contrastar el modelo peruano con experiencias internacionales, como el Reglamento de la Unión Europea (AI Act) o las directivas canadienses y brasileñas, se observa un claro rezago normativo. Mientras otras jurisdicciones han establecido estándares exigibles de supervisión, clasificación de riesgos y control democrático de la IA, la Ley N.º 31814 carece incluso de un reglamento operativo, lo que incrementa su carácter programático y la convierte en una norma de aspiración más que de efectividad.

Por ello, el presente artículo concluye que es urgente la adopción de una regulación especializada sobre inteligencia artificial judicial, que parta de los siguientes principios:

- El respeto irrestricto de la dignidad humana como límite a toda automatización.
- La primacía del juicio humano prudencial sobre cualquier herramienta tecnológica.
- La obligación de garantizar trazabilidad, explicabilidad, participación y posibilidad de revisión.
- La incorporación de una evaluación de impacto ético-jurídico ex ante y ex post en todo sistema algorítmico aplicado al ámbito judicial.

Sin estos elementos, la justicia digital corre el riesgo de convertirse en una “justicia sin rostro”, en la que la persona desaparece tras el velo de la técnica. Frente a ello, el Estado tiene el deber de asegurar que toda transformación tecnológica se subordine a los fines superiores del derecho: la equidad, la racionalidad práctica, y la centralidad de la persona como sujeto de derechos y no como objeto de procesamiento algorítmico.

El derecho a reusar los datos personales ante las entidades del sector público*

Gabriela Guadalupe Bolaños Vainstein**, Rosa Isabel Espinoza
Córdova*** y Ana Lucia Taboada Cardenas****

Resumen.- El artículo analiza si la reutilización de datos personales, a través de la portabilidad, puede ser exigible a entidades públicas peruanas. Examina los conceptos de portabilidad e interoperabilidad, normativas vigentes, servicios digitales públicos y privados, y el nuevo Reglamento de la Ley N.º 29733, proponiendo una interpretación alineada con el régimen de protección de datos personales en el ámbito público.

Palabras clave.- Datos personales – autodeterminación informativa – portabilidad – interoperabilidad – transformación digital – gobierno digital – servicios digitales – ciudadanía digital.

Abstract.- The article examines whether the reuse of personal data, through portability, can be required of Peruvian public entities. It analyzes the concepts of portability and interoperability, current regulations, public and private digital services, and the new Regulation of Law No. 29733, proposing an interpretation aligned with the personal data protection regime in the public sector.

Keywords.- Personal data – informational self-determination – portability – interoperability – digital transformation – digital government – digital services, digital citizenship.

* Agradecemos a Alejandro Morales Cáceres, Anais C. Zavala Huaisara, Yuri Aldoradín Carbajal, Alexandra Párraga Cardozo, y Fredy Otárola Peñaranda quienes contribuyeron en esta investigación.

** Abogada por la Universidad de Lima, especializada en protección de datos, tecnología y seguridad de la información. Becaria Ian R. Kerr en la Universidad de Ottawa y cursa Máster en Derecho y Tecnología. Certificada por IAITG, con estudios en LSE y Bayreuth.

*** Abogada summa cum laude por la Universidad de Lima con diploma en Solución de Controversias. Representó a su universidad en competencias internacionales de arbitraje. Especialista en Derecho Procesal Civil. Abogada del área de litigios y controversias en el Estudio Muñiz.

**** Abogada por la Universidad del Pacífico con mención Sobresaliente. Certificada en Protección de Datos por IAITG, con estudios en LSE y Uniandes. Fellow de YouthLACIGE, South School of Internet y Escuela de Gobernanza de Argentina. Cofundadora de La Cápsula. Legal Manager en Laboratorios Diphasac.

I. Introducción

Desde el año 2019, la Organización para la Cooperación y el Desarrollo Económicos [OCDE]¹ reconoció que destinar esfuerzos a potenciar el acceso y el intercambio de datos entre países puede generar importantes beneficios sociales y económicos. Los datos compartidos pueden ser hasta 50 veces más valiosos que los datos aislados, contribuyendo entre un 0,5 % y un 1,2 % del Producto Bruto Interno (PBI) nacional, en particular al impulsar la productividad y la innovación en empresas de alto rendimiento².

Más allá de estos beneficios económicos, el acceso a los datos fortalece el valor público al apoyar la investigación, mejorar los servicios públicos e informar la formulación de políticas. La pandemia de la COVID-19 ilustró esto de manera vívida, ya que el intercambio oportuno y seguro de datos permitió la coordinación sanitaria, el desarrollo de vacunas y la cooperación global.

Asimismo, en respuesta a esta brecha, en octubre de 2021 el Consejo de la OCDE adoptó formalmente un instrumento jurídico oficial: la *Recomendación del Consejo sobre el Fomento del Acceso y la Compartición de Datos*³, un instrumento no vinculante destinado a asistir a los Miembros de la OCDE y a las economías asociadas que se adhieran en el diseño de marcos normativos que promuevan una economía basada en datos y abordar los riesgos asociados. En lugar de centrarse únicamente en la

¹ Organización para la Cooperación y el Desarrollo Económico [OCDE]. (2019). *Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies*. OECD Publishing.

² Según la UNCTAD (2021), destaca que los flujos de datos digitales transfronterizos pueden impulsar el desarrollo económico, permitiendo que los países aprovechen los datos como un bien público global y fomentando la innovación y el progreso económico.
UNCTAD. (2021). *La UNCTAD hace un llamado para que los flujos de datos digitales sean de beneficio económico global*. Conferencia de las Naciones Unidas sobre Comercio y Desarrollo.

³ OECD, *Recommendation of the Council on Enhancing Access to and Sharing of Data*, OECD/LEGAL/0463 (Paris: OECD Publishing, 2021), online: <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0463>.

divulgación, la Recomendación enfatiza la importancia de la confianza, la interoperabilidad y la generación de valor público a partir de los datos.

En 2025 se aprobó un documento complementario que busca poner en práctica la Recomendación mediante siete principios generales, organizados en tres grandes áreas. La primera se centra en cómo se gestionan y coordinan las instituciones (principios 1 y 2), la segunda promueve el uso responsable de los datos para fomentar la innovación (principio 3), y la tercera destaca la importancia de la interoperabilidad y el fortalecimiento de capacidades técnicas (principios 6 y 7). En conjunto, estos principios no deben entenderse como reglas sueltas, sino como parte de un enfoque integral que responde a los avances en inteligencia artificial, sus desafíos y la necesidad de una gobernanza colaborativa entre distintos actores⁴.

Este marco internacional muestra una tensión importante: por un lado, se busca que los datos sean más accesibles, reutilizables e interoperables para fomentar la innovación y generar valor público; pero por otro lado, las normas de protección de datos de datos personales deben asegurarse de proteger los derechos de las personas. En ese contexto, el derecho a la portabilidad enfrenta el reto de encontrar un equilibrio entre permitir que los datos se usen de forma útil y, al mismo tiempo, asegurar que las personas mantengan el control sobre su información, incluso cuando esta se encuentra en manos del Estado.

Es así que, en el marco del proceso de adhesión del Perú a la OCDE, el Decreto Supremo No. 016-2024-JUS, publicado el 30 de noviembre de 2024, introdujo el nuevo Reglamento de la Ley No. 29733, Ley de Protección de Datos Personales (en adelante, el “Reglamento”), modificando integralmente la normativa previa con el propósito de alinear el marco normativo peruano con estándares internacionales y responder a las necesidades contemporáneas en materia de protección de datos personales, especialmente en contextos tecnológicos avanzados.

⁴ OECD, *Enhancing Access to and Sharing of Data in the Age of Artificial Intelligence: Companion Document to the OECD Council Recommendation on Enhancing Access to and Sharing of Data*, COM/DSTI/CDEP/STP/GOV/PGC(2024)1/FINAL (Paris: OECD Publishing, 2025) at 5, online.

Entre las principales novedades, se destaca la incorporación del ejercicio del derecho a la portabilidad de datos personales, un hito significativo en el camino hacia la digitalización del país. Sin embargo, este nuevo derecho no se aplica cuando los datos son tratados por entidades públicas. para cumplir con sus funciones o responsabilidades. Así, surge la siguiente interrogante: ¿cuál debería ser el alcance de este derecho? ¿Puede o debe interpretarse esta redacción como una limitación en su aplicación frente a las entidades públicas, como parecería haberse sugerido preliminarmente en la Exposición de Motivos del Proyecto de Reglamento⁵?

En este contexto, y ante la entrada en vigor de este derecho, resulta fundamental determinar si el derecho a la portabilidad de datos personales podría ser exigible y oponible frente a las entidades públicas peruanas en el ejercicio de sus competencias. De ser ello posible, es necesario establecer bajo qué presupuestos o condiciones podría configurarse de manera coherente y armoniosa con el ordenamiento jurídico vigente.

Por lo tanto, esta investigación tiene como objetivo analizar y esclarecer dicha disposición con el fin de promover la implementación efectiva de este nuevo derecho en entornos digitales, garantizando su compatibilidad con las competencias y funciones de la Administración Pública peruana en la materia.

II. ¿Qué son la portabilidad y la interoperabilidad?

i. La portabilidad

La portabilidad, según la norma ISO/IEC 25000:2014⁶ es la capacidad de un producto o componente para ser transferido eficientemente

⁵ Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales. (2023). Exposición de Motivos de la Resolución 0270-2023-JUS, “Proyecto de Reglamento a la Ley N° 29733, Ley de Protección de Datos Personales”. <https://cdn.www.gob.pe/uploads/document/file/5050225/expo%20de%20motivos.pdf?v=1693066494>

⁶ International Organization for Standardization & International Electrotechnical Commission. (2014). *ISO/IEC 25000:2014 Systems and Software Engineering – Systems and Software Quality Requirements and Evaluation (Square) – Guide to Square* [Ingeniería de Sistemas y Software - Requisitos y Evaluación de Calidad de Sistemas y Software (Cuadrado) - Guía De Cuadrado]. <https://www.iso.org/standard/64764.html>

entre diferentes entornos de hardware, software o uso operativo, incluyendo su adaptabilidad, facilidad de instalación y reemplazo. Complementariamente, la norma ISO/IEC 17788:2014⁷ define a la portabilidad como la capacidad de transferir datos de un sistema a otro sin necesidad de ingresarlos manualmente, asegurando que la conversión entre formatos sea posible con herramientas disponibles, facilitando así un traslado efectivo entre sistemas.

Desde el año 2019, la Organización para la Cooperación y el Desarrollo Económicos [OCDE]⁸ reconoció que destinar esfuerzos a potenciar el acceso y el intercambio de datos entre países puede generar importantes beneficios sociales y económicos⁹. Estos esfuerzos se enmarcan, según la doctrina y las políticas públicas de gobiernos a nivel global¹⁰, en

⁷ International Organization for Standardization & International Electrotechnical Commission. (2014). *ISO / IEC 17788: 2014(en). Tecnología de la información - Computación en la nube - Descripción general y vocabulario*. <https://www.iso.org/obp/ui/#iso:std:iso-iec:17788:ed-1:v1:en>

⁸ Organización para la Cooperación y el Desarrollo Económico [OCDE]. (2019). *Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies*. OECD Publishing.

⁹ Según la UNCTAD (2021), destaca que los flujos de datos digitales transfronterizos pueden impulsar el desarrollo económico, permitiendo que los países aprovechen los datos como un bien público global y fomentando la innovación y el progreso económico.

UNCTAD. (2021). La UNCTAD hace un llamado para que los flujos de datos digitales sean de beneficio económico global. Conferencia de las Naciones Unidas sobre Comercio y Desarrollo. <https://unctad.org/es/press-material/la-unctad-hace-un-llamado-para-que-los-flujos-de-datos-digitales-sean-de-beneficio>

¹⁰ El primer enfoque es denominado *Open Access*. Es el más utilizado para mejorar el acceso (apertura) a los datos (OCDE, 2015) y ha sido satisfactoriamente empleado en el sector público. Los datos gubernamentales abiertos han sido promovidos por iniciativas, como *data.gov*, en Estados Unidos; *data.gov.uk*, en Reino Unido; *data.gov.fr*, en Francia; y, *data.go.jp*, en Japón.

Otros ejemplos incluyen a X-Road® en Estonia, que es una solución de software de código abierto y un ecosistema que facilita un intercambio de datos seguro y unificado entre organizaciones del sector público y privado (OECD, 2024, p. 45).

Igualmente, desde 2010, en los Estados Unidos, iniciativas como Blue Button y Green Button han evolucionado para ofrecer a los consumidores un mayor control sobre sus datos personales. Ambas iniciativas han avanzado la portabilidad de datos 2.0 y 3.0, facilitando el acceso a datos y fomentando la innovación, aunque son voluntarias para las organizaciones (OECD, 2024, pp. 39-40).

enfoques relacionados con los datos abiertos, los mercados de datos y la portabilidad de datos. Ante ello, los gobiernos y entidades internacionales vienen promoviendo diversas iniciativas en los sectores público y privado para cumplir dicha recomendación.

Según la OCDE (2021)¹¹, las iniciativas dentro del enfoque de portabilidad de datos adoptadas a nivel global varían significativamente entre jurisdicciones en términos de naturaleza, propósito, alcance (es decir, quién tiene el derecho a la transferencia de datos y qué datos pueden ser transferidos), requisitos técnicos y legales, y su implementación. No obstante, se identifican cinco (5) dimensiones comunes para estas iniciativas¹²:

- **Alcance sectorial:** Si son específicas para un sector o abarcan todos los titulares de datos en diferentes sectores.
- **Beneficiarios:** Si solo personas naturales (individuos) o también personas jurídicas (empresas) tienen derecho a la portabilidad de datos.
- **Tipo de datos:** Si se limita a datos personales o incluye datos voluntarios, observados o derivados.
- **Obligaciones legales:** Si la portabilidad es voluntaria u obligatoria, y si se basa en medidas regulatorias ex ante (preventivas) o ex post (remedios tras violaciones).

E-Estonia. (s.f.). *X-Road: Servicios de interoperabilidad*. <https://e-estonia.com/solutions/x-road-interoperability-services/x-road/>

¹¹ Organización para la Cooperación y el Desarrollo Económico [OCDE]. (2021). *Mapping data portability initiatives, opportunities and challenges*.

¹² Pese a ello, la OECD (2021) reconoce que la implementación de la portabilidad de datos enfrenta varios desafíos. Existe incertidumbre sobre el alcance de las iniciativas, como qué datos pueden transferirse y quién tiene derecho a ello. También hay preocupaciones sobre seguridad y privacidad, ya que liberar el flujo de datos puede incrementar riesgos. La falta de estándares y APIs interoperables puede complicar la implementación, y los costos de cumplimiento, aunque suelen ser gastos únicos, pueden incluir costos técnicos y legales. Además, se requiere una coordinación efectiva entre agencias regulatorias para manejar las iniciativas de manera eficiente.

- **Modalidad operativa:** Si los datos se transfieren de manera ad hoc en formatos legibles por máquina (portabilidad 1.0), mediante transferencias directas a otro titular (portabilidad 2.0), o en tiempo real (transferencias continuas).

A pesar de estas variaciones, los conceptos de portabilidad e interoperabilidad¹³ están estrechamente relacionados¹⁴ y juegan un papel clave en la transformación digital de ecosistemas públicos y privados, particularmente en la provisión de servicios digitales.

ii. La interoperabilidad

Respecto a la interoperabilidad, esta se define como la capacidad de dos o más sistemas o aplicaciones para intercambiar información y utilizarla mutuamente (ISO/IEC 17788:2014, 3.1.5)¹⁵. De manera similar, la Secretaría de Gobierno y Transformación Digital de la Presidencia

¹³ Hoffman y Gonzalez (2020) señalan que la interoperabilidad, al igual que la apertura, se considera positiva porque permite que sistemas, productos o servicios diferentes se comuniquen y funcionen juntos, fomentando así la innovación y la competencia. Sin embargo, un desafío importante es definir el nivel óptimo de interoperabilidad y cómo deben interactuar estos sistemas. Además, no hay una definición uniforme de interoperabilidad, ya que depende del contexto de leyes, políticas y tecnologías, donde los estándares son cruciales y pueden afectar el acceso a los datos (Hoffman & Gonzalez, 2020, pp. 255-256).

Los autores también diferencian entre interoperabilidad sintáctica, que se refiere a la compatibilidad del formato y la estructura de datos (como *WSDL* y *APIs RESTful*), y la interoperabilidad semántica, que implica un intercambio significativo de información, esencial para la innovación basada en datos. Sin embargo, esta última no está suficientemente abordada en los marcos regulatorios actuales, lo que limita la innovación y la eficiencia en la gobernanza de datos (Hoffman & Gonzalez, 2020, pp. 257-258).

HOFFMANN, J., & OTERO, B. (2021). Demystifying the role of data interoperability in the access and sharing debate. *JIPITEC*, 11(3), 252. <https://www.jipitec.eu/archive/issues/jipitec-11-3-2020/5187>

¹⁴ La portabilidad se centra en el movimiento físico o digital de la información. Por otro lado, la interoperabilidad se enfoca en garantizar que la información sea comprensible y utilizable en su destino final.

¹⁵ International Organization for Standardization & International Electrotechnical Commission. (2014). *ISO / IEC 17788: 2014(en). Tecnología de la información - Computación en la nube - Descripción general y vocabulario*. <https://www.iso.org/obp/ui/#iso:std:iso-iec:17788:ed-1:v1:en>

del Consejo de Ministros [SGTD] (2018) sostiene que es “la habilidad de organizaciones y sistemas dispares y diversos para interactuar con objetivos consensuados y comunes, con la finalidad de obtener beneficios mutuos. La interacción implica que las organizaciones involucradas compartan información y conocimiento a través de sus procesos de negocio, mediante el intercambio de datos entre sus respectivos sistemas de Tecnologías de la Información y Comunicaciones (TIC)”.

Aunando en ello, Crémer, de Montjoye y Schweitzer (2019)¹⁶ identifican tres tipos de interoperabilidad:

- **Interoperabilidad de protocolos o sistemas:** Permite la interconexión técnica entre servicios o productos, aplicada en políticas de competencia europeas.
- **Interoperabilidad de datos:** Equivalente a la portabilidad de datos, pero con acceso continuo y potencialmente en tiempo real.
- **Interoperabilidad de protocolo completo:** Establece estándares para que servicios sustitutos puedan interoperar, como en los sistemas de mensajería.

Estos tres tipos de interoperabilidad pueden ilustrarse mediante la analogía del traslado de documentos entre oficinas físicas. Nos explicamos: La interoperabilidad de protocolos o sistemas sería comparable a garantizar que dos oficinas puedan conectarse y aceptar un documento, a pesar de tener diferentes sistemas de seguridad y normas sobre cómo recibir y enviar documentos.

Por otro lado, la interoperabilidad de datos asegura que la información en el documento esté en un formato y lenguaje que la oficina receptora pueda leer, como un texto impreso en español. Por último, la interoperabilidad de protocolo completo sería como si todas las oficinas estuvieran conectadas directamente, permitiendo el envío de documentos sin necesidad de trasladarlos físicamente, simplificando el proceso y eliminando la necesidad de verificar cada paso por separado.

Así como la interoperabilidad entre oficinas físicas dentro de una misma sede simplifica el traslado de documentos, en entornos digitales

¹⁶ CRÉMER, J., DE MONTJOYE, Y.A. & SCHWEITZER, H. (2019). *Competition policy for the digital era*. Comisión Europea. <https://doi.org/10.2763/407537>

facilita la transferencia instantánea de datos entre diferentes sistemas y plataformas, lo que mejora la eficiencia operativa y la experiencia del usuario, promoviendo una mayor conectividad y colaboración.

Ante ello, el Decreto Legislativo N° 1412, Ley de Gobierno Digital¹⁷, desarrolla el Marco de Interoperabilidad del Estado Peruano, el cual advierte, en su artículo 27°, su conformación a través de políticas, lineamientos, especificaciones, estándares e infraestructura de tecnologías digitales, que permiten, de manera efectiva, la colaboración entre entidades públicas para el intercambio de información y conocimiento, el ejercicio de sus funciones en el ámbito de sus competencias y la prestación de servicios digitales interadministrativos de valor para el ciudadano en canales digitales. Para ello, en el artículo 28, se detallan los niveles para su gestión.

En ese sentido, como señala el Foro Económico Mundial (2023)¹⁸, la interoperabilidad no solo se debe considerar desde un punto de vista técnico, sino también en términos de uso y normas en diferentes regiones. Es esencial establecer medidas de seguridad y fomentar la colaboración en la gestión, ya que esto influye en cómo se toman las decisiones, en la participación y en el diseño de datos e infraestructura. La interoperabilidad ayuda a mejorar el acceso a experiencias digitales y mercados, a crear beneficios en áreas como la privacidad y la seguridad, y a ofrecer nuevas formas de disfrutar las experiencias de la vida real para los usuarios (p. 6).

De estas reflexiones iniciales sobre la relación entre la interoperabilidad y la portabilidad de datos, podemos destacar varios puntos claves. Entre ellos, que la portabilidad implica la transferencia fácil y eficiente de datos sin la necesidad de reintroducir la información para garantizar su reutilización; requiere el uso de formatos o estándares comunes¹⁹ y

¹⁷ Decreto Legislativo N° 1412, Decreto legislativo que aprueba la Ley de Gobierno Digital. (13 de setiembre de 2018).

¹⁸ Foro Económico Mundial. (2024). *Interoperabilidad en el metaverso*. World Economic Forum.

¹⁹ En el contexto de la interoperabilidad, los estándares proporcionan orientación sobre cómo, cuándo y dónde se debe utilizar, o no utilizar, la interoperabilidad. La ausencia de estándares puede llevar a sistemas fragmentados (Foro Económico Mundial, 2023, p.6).

está estrechamente relacionada con la interoperabilidad, siendo que esta última puede servir como una condición habilitante para la portabilidad a nivel de los datos. Además, su implementación exitosa depende de la colaboración entre los diferentes actores involucrados, y tiene implicaciones significativas en la seguridad y confidencialidad.

III. Implicancias legales de la portabilidad e interoperabilidad

i. Portabilidad y su impacto en la autodeterminación informativa

En base al acápite anterior, es necesario explicar la conexión entre la portabilidad y la dignidad humana, la cual está, a su vez, inmersa en el derecho fundamental de la autodeterminación informativa.

En la actualidad, existe consenso en que la autodeterminación informativa es un derecho fundamental, subjetivo, autónomo y facilitador de otros derechos básicos de la personalidad, que a su vez se sustentan en el derecho a la dignidad humana²⁰. Su naturaleza relacional o facilitadora implica que las exigencias para garantizar su respeto estén frecuentemente vinculadas a la protección de otros derechos constitucionales, tales como la privacidad, honor, intimidad, etc.

El Tribunal Constitucional del Perú ha reconocido en diversas sentencias, como los expedientes 06164-2007-PHD-TC²¹, 04227-2009-PHD/TC²² y,

Foro Económico Mundial. (2024). *Interoperabilidad en el metaverso*. World Economic Forum.

²⁰ El derecho a la autodeterminación informativa está reconocido en el artículo 2.6 de la Constitución Política del Perú (1993), el cual dispone que “los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar”. Este derecho fue enunciado por primera vez jurisprudencialmente en el fundamento 3 de la Sentencia 1797-2002-HD/Tribunal Constitucional.

Tribunal Constitucional. Sala Primera. Expediente N° 1797-2002-HD/TC, Lima, Wilo Rodríguez Gutiérrez. (29 de enero de 2003).

²¹ Tribunal Constitucional. Expediente N° 06164-2007-HD/TC, Arequipa, Jhonny Robert Colmenares Jiménez. (21 de diciembre de 2007).

²² Mediante dicha sentencia, el TC (2007) en una función pedagógica, dictaminó los distintos tipos de hábeas data existentes.

Tribunal Constitucional. Sala Primera. Expediente N° 04227-2009-PHD/TC, Arequipa, Jhonny Robert Colmenares Jiménez. (30 de mayo de 2011).

más recientemente, la 238/2022-PHD/TC²³, que el derecho a la autodeterminación informativa forma parte del contenido protegido por el hábeas data.

Según su interpretación, este derecho otorga a toda persona la facultad de controlar su información personal registrada en bases de datos públicas, privadas o informáticos. (Tribunal Constitucional. Expediente 4739-2007-PHD/TC, Lima, Pesquera Virgen del Valle S.A.C.; 15 de octubre de 2007)²⁴. Este control abarca cómo se recopilan, usan y divulgan sus datos, garantizando así que cada individuo pueda decidir sobre el manejo de su propia información.

Además, en la Sentencia 00693-2012-PHD/TC²⁵, el TC (2012) estableció que toda persona tiene derecho a hacer uso, por sí misma, de los datos personales que terceros públicos o privados tengan en su poder. Por ello, la autodeterminación informativa también implica el obtener copia de los datos personales tal como se transcribe a continuación:

La autodeterminación informativa también supone que una persona pueda hacer uso de la información privada que existe sobre ella (...) una persona tiene derecho a obtener copia de la información particular que le concierne, al margen de si ésta se encuentra disponible en una entidad pública o privada [Énfasis añadido].

Prueba de ello es que, como parte de las facultades de control previstas en el derecho a la autodeterminación informativa, la Ley N° 29733, Ley de Protección de Datos Personales (2011) [LPDP]²⁶, establece que todo titular de datos personales goza de once (11) derechos.

En este contexto, el artículo 76 del nuevo Reglamento reconoce que el derecho a portar los datos personales constituye una manifestación del derecho de acceso. Según lo estipulado, “el titular del dato puede solicitar los datos personales sobre sí mismo, que haya facilitado (...) en un

²³ Tribunal Constitucional. Expediente N° 02839-2021-HD/TC, Lima, Sebastián Carlos Aguedo Zúñiga. (22 de agosto de 2022).

²⁴ Tribunal Constitucional. Sala Primera. Expediente N° 04739-2007-PHD/TC, Lima, Pesquera Virgen Del Valle S.A.C. (15 de octubre de 2007).

²⁵ Tribunal Constitucional. Sala Primera. Expediente N° 00693-2012-PHD/TC, Lambayeque, José Manuel Curipuma Alburqueque. (24 de julio de 2012).

²⁶ Ley N° 29733, Ley de Protección de Datos Personales. (03 de julio de 2011).

formato estructurado, de uso común y lectura mecánica, y transmitirlos a otro responsable o titular de banco de datos personales” bajo ciertas circunstancias o condiciones.

Sin embargo, el inciso 6 del mismo artículo introduce una limitación relevante: excluye la aplicación de este derecho cuando el tratamiento de los datos personales sea necesario para el ejercicio de competencias o funciones asignadas a entidades públicas. Pese a ello, se prevé que la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales (DGTAIPD) pueda emitir disposiciones adicionales para guiar cómo se aplica este derecho en la práctica, lo que significa que esta limitación podría entenderse de forma flexible, dependiendo del contexto.

Como se indicó, en el plano constitucional y legal, la facultad de control del acceso —y otras relacionadas— debiera operar independientemente del tipo de responsable del tratamiento, del soporte utilizado o del tipo de tratamiento empleado. Esta afirmación también se alinea con lo dictaminado por la Red Iberoamericana de Protección de Datos Personales (RIPD), la DGTAIPD y la Agencia Española de Protección de Datos (AEPD)²⁷, las cuales sostienen que “la regulación del tratamiento de datos personales debe aplicarse al margen de los procedimientos, metodologías o mecanismos que se utilicen para recolectar, usar o tratar los datos personales”.

De acuerdo con estas instituciones, toda normativa sobre tratamiento de datos debe ser “neutral temática y tecnológicamente”; es decir, debe aplicarse a cualquier tratamiento de datos, independientemente de las técnicas, procesos o tecnologías actuales o futuras utilizadas (Reglamento, p.20).

Desde una perspectiva constitucional, se reconoce que este derecho incluye el uso de la información privada, así como la obtención de una copia de la misma. En este sentido, la portabilidad permite que los datos sean transmitidos y reutilizados con mayor facilidad por diferentes

²⁷ Agencia Española de Protección de Datos. (2021). *Instrucción 1/2021, de 2 de noviembre, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales en relación con la obligación de transparencia activa*. Boletín Oficial del Estado, núm. 266, de 6 de noviembre de 2021. Recuperado de <https://www.boe.es/buscar/act.php?id=BOE-A-2021-18134>

responsables del tratamiento, alineándose con los avances tecnológicos y las dinámicas de la economía digital²⁸.

No obstante, para promover su implementación y otorgar mayor autonomía a los titulares de los datos, varias legislaciones, como las de la Unión Europea²⁹ y otros países latinoamericanos, han incorporado la portabilidad como un derecho nuevo e independiente, aunque estrechamente vinculado y dependiente del derecho de acceso³⁰.

De esta forma, el nuevo Reglamento busca atender la necesidad de contar con un mecanismo específico que reconozca la facultad de portar datos

²⁸ En palabras de la propia DGTAIPD (2023), se considera que la inclusión de la portabilidad de datos personales contribuye “al nivel adecuado de protección de datos en el país, sino que también estaría en línea con estándares internacionales, como los Principios Actualizados del Comité Jurídico Interamericano sobre Privacidad y Protección de Datos Personales de la OEA, el Reglamento General de Protección de Datos de la UE, y los Estándares en Protección de Datos Personales para los Estados Iberoamericanos.

²⁹ Al respecto, Li (2018) cuenta que esta proximidad entre ambos derechos se refleja incluso en la historia legislativa, pues la Comisión Europea declaró inicialmente que el derecho a la portabilidad de datos personales sirve como condición previa y para mejorar aún más el acceso de las personas. El Grupo de Trabajo del Artículo 29 (2017) incluso reconoce que el nuevo derecho a la portabilidad de datos personales está estrechamente relacionado con el derecho de acceso, pero se diferencia de él en muchos aspectos; complementa el derecho de acceso sobre todo al eliminar la restricción del formato de datos.

European Commission. (2017, April 13). Guidelines on the right to data portability (WP 242). Article 29 Working Party. https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233.

Grupo de trabajo sobre protección de datos del Artículo 29 [GT 242 rev.01]. (5 de abril de 2017). Directrices sobre el derecho a la portabilidad de los datos. https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233

Li, W. (2018). A tale of two rights: exploring the potential conflict between right to data portability and right to be forgotten under the General Data Protection Regulation. *International Data Privacy Law*.

³⁰ Como comentan Kranz et al. (2023), regulaciones similares han sido adoptadas en California con la Ley de Privacidad del Consumidor de California, en China en el Artículo 45 de su Ley de Protección de Información Personal, y en India y Brasil dentro de su Proyecto de Ley de Protección de Datos Personales y la Ley General de Protección de Datos Personales, entre otros (p. 598).

Kranz, J., Kuebler-Wachendorff, S., Symoudis, E. et al. Data Portability. *Bus Inf Syst Eng* 65, 597–607 (2023). <https://doi.org/10.1007/s12599-023-00815-w>

personales en entornos digitales, junto con las excepciones, presupuestos y condiciones técnicas necesarias para garantizar su reutilización³¹.

Ahora bien, al contrastar el texto aprobado por el Reglamento se observa que en gran medida se alinea a los estándares recomendados por la RIPD (2017). Sin embargo, la inoponibilidad de este derecho ante las competencias del sector público pareciera ser una adición local inspirada en algunas otras legislaciones comparadas como la europea del artículo 20 del Reglamento UE 2016/679, que dispone que este derecho no es aplicable al *“processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller”*. Lo anterior, sin perjuicio de la amplia normativa existente en dicho territorio en materia de interoperabilidad.

De igual forma, cabe indicar que los estándares de la RIPD (2017), con carácter orientativo, de la cual el Perú es país miembro, no distingue específicamente entre ambos tipos de responsables de tratamiento ni en el ámbito de aplicación de la propuesta legislativa, ni en la aplicación específica de este derecho³².

³¹ Para ejercer este derecho, es necesario que los datos sean tratados mediante medios automatizados y hayan sido proporcionados por el titular o generados en el marco de una relación contractual o mediante consentimiento. Los datos derivados o inferidos solo serán portables si el responsable del tratamiento lo permite. Además, la portabilidad no debe afectar derechos de terceros, como la privacidad o la propiedad intelectual. Y se excluye de la portabilidad aquellos tratamientos necesarios para cumplir funciones o competencias de entidades públicas.

Tomar en cuenta que el término “facilitar” abarca tanto datos proporcionados activamente, como los registrados en formularios, como aquellos recolectados indirectamente durante el uso de un servicio digital. En casos de datos derivados o inferidos, aunque su portabilidad queda a discreción del responsable, se sugiere incentivar su inclusión siempre que no se vulneren derechos de terceros. Sin embargo, cuando no sea posible, el titular puede ejercer otros derechos, como solicitar acceso o información sobre decisiones automatizadas que lo afecten.

Los datos anonimizados quedan fuera de este derecho, pero no así los disociados que aún puedan vincularse con su titular. Respecto a datos relacionados con terceros, no podrán portarse si afectan sus derechos, salvo que exista un debido consentimiento para ello. Para evitar conflictos, se recomienda implementar herramientas que permitan recabar dicho consentimiento y proteger derechos mediante mecanismos claros de autenticación, así como protocolos de seguridad robustos, como cifrado de extremo a extremo y medidas de mitigación de riesgos.

³² 30.1. Cuando se traten datos personales por vía electrónica o medios automatizados, el titular tendrá derecho a obtener una copia de los datos personales que hubiere

Si bien el artículo 32 (RIPD, 2017) detalla las causales de improcedencia con respecto a la totalidad de todos los derechos de los titulares de datos personales, sin especificar ni prohibir su aplicación ante el sector público.

Si bien dicho estándar internacional es un marco orientativo que debe adaptarse y desarrollarse conforme a la realidad de cada país miembro, en el Perú la LPDP se aplica por igual a entidades públicas y privadas. Tanto el análisis constitucional y legal como los criterios de la RIPD (2017) evidencian que el marco reglamentario vigente no debería establecer distinciones al momento de exigir el cumplimiento de las obligaciones de portabilidad, por lo que los derechos de los titulares de datos personales –incluida su oponibilidad– resultan exigibles también frente a las entidades públicas.

ii. Interoperabilidad y acceso a servicios públicos digitales

Como ya se ha señalado, la interoperabilidad es la capacidad de interactuar que tienen las organizaciones diversas y dispares para alcanzar objetivos que hayan acordado conjuntamente (Decreto Legislativo N° 1412, 2018)³³. En otras palabras, la interoperabilidad se configura como la capacidad de transferencia de información y conocimiento entre diversos sistemas y organizaciones, a través de la comunicación e intercambio mutuo de datos. (Espinoza & López, 2022)³⁴.

En un primer momento, la interoperabilidad fue utilizada en el plano internacional como herramienta para compartir información estratégica

proporcionado al responsable o que sean objeto de tratamiento, en un formato electrónico estructurado, de uso común y lectura mecánica, que le permita seguir utilizándolos y transferirlos a otro responsable, en caso de que lo requiera.

30.2. El titular podrá solicitar que sus datos personales se transfieran directamente de responsable a responsable cuando sea técnicamente posible.

30.3. El derecho a la portabilidad de los datos personales no afectará negativamente a los derechos y libertades de otros.

³³ Decreto Legislativo N° 1412, Decreto legislativo que aprueba la Ley de Gobierno Digital. (13 de setiembre de 2018).

³⁴ ESPINOZA, R. & LOPEZ, M. (2022). La limitación de derechos fundamentales y principios procesales en la tradicional impartición de justicia durante el proceso judicial en el Perú y la necesaria incorporación de la digitalización y las tecnologías de la información y las comunicaciones [Tesis para optar el título profesional de Abogado, Universidad de Lima]. Repositorio institucional de la Universidad de Lima. <https://hdl.handle.net/20.500.12724/17221>

en el marco militar. No obstante, los usos de la interoperabilidad se fueron expandiendo a otras áreas. Por ejemplo, en el año 2004, la Comunidad Europea implementó un marco de interoperabilidad denominado “*Communication Online Data Exchange*” (e-CODEX) (Salazar-Pimpincos & Sánchez) donde, gracias a la colaboración de los distintos poderes judiciales y la policía de cada país, se pudo intercambiar información para identificar de manera oportuna a personas que se encontraban desaparecidas o prófugas.

En el plano nacional, el artículo 28 de la Ley de Gobierno Digital contempla una rúbrica de dimensiones y niveles que permiten a cada entidad pública determinar en qué nivel de interoperabilidad se encuentra. Para ello, las dimensiones son las siguientes:

Organizacional	Semántica	Técnica	Legal
Enfocado en el alineamiento de objetivos, procesos, responsabilidades y relaciones entre las entidades públicas para intercambiar datos e información para el ejercicio de sus funciones.	Relativa al uso de los datos y a la información de una entidad, garantizando que el formato y significado preciso de dichos datos e información a ser intercambiada puedan ser entendidos por cualquier aplicación de otra entidad pública. Por ello, deben adoptar los estándares definidos por el ente rector para el intercambio de datos e información.	Sobre aspectos técnicos relacionados con las interfaces, la interconexión, integración, intercambio y presentación de datos e información. También, define los protocolos de comunicación y seguridad necesarios. Es ejecutado por personal de las oficinas de informática de las entidades públicas, de acuerdo a los estándares definidos por el ente rector.	Busca la adecuada observancia de la legislación y lineamientos técnicos para facilitar el intercambio de datos e información entre las entidades públicas y el tratamiento de la información intercambiada.

Fuente: Elaboración propia

Tales dimensiones se alinean a los estándares internacionales en la materia, conforme al Libro Blanco de Interoperabilidad de Gobierno

Electrónico para América Latina y el Caribe (Comisión Económica para América Latina y El Caribe [CEPAL], 2007)³⁵. Asimismo, una vez que se analiza el cumplimiento de las dimensiones, se puede conocer en cuál de los tres (3) niveles de madurez de interoperabilidad se encuentra la entidad: (i) Inicial, (ii) Definido y (iii) Optimizado.

A fin de garantizar la transformación digital en el país en la provisión de servicios públicos y funciones de las distintas entidades del gobierno a nivel nacional, la SGTD es el ente técnico-normativo en la transformación digital del país³⁶ en el marco del “Sistema Nacional de Transformación Digital”. Con ello, las materias comprendidas por la transformación digital son la ciudadanía digital, la economía digital, el gobierno digital, el talento digital, la seguridad y confianza digital, las tecnologías digitales, la innovación digital, y servicios digitales (Decreto de Urgencia N° 006, 2020).

De acuerdo con la Opinión Técnica Vinculante N° 001-2024-PCM-SG-SGTD³⁷, la SGTD (2024) precisa que las materias comprendidas en sus funciones comprenden la adopción y el uso estratégico de la gestión de identidad digital, interoperabilidad, seguridad digital y arquitectura digital del Estado. De igual manera, recalca que “supervisa y gestiona proyectos digitales transversales, colaborando con otros sectores según sea necesario”.

Ante ello, un proyecto digital transversal es aquel que desarrolla plataformas o servicios digitales usados por varias entidades públicas. Estos proyectos deben cumplir con ciertos criterios: abordar objetivos estratégicos nacionales, integrarse con bloques de interoperabilidad

³⁵ Comisión Económica para América Latina y el Caribe. (2007). *Libro Blanco de Interoperabilidad de Gobierno Electrónico para América Latina y el Caribe*. <https://repositorio.cepal.org/server/api/core/bitstreams/ec93d026-91b1-4d7e-9e9e-00d16b351fcb/content>

³⁶ Esto es, todo “proceso continuo, disruptivo, estratégico y de cambio cultural que se sustenta en el uso intensivo de las tecnologías digitales, sistematización y análisis de datos para generar efectos económicos, sociales y de valor para las personas”. (Decreto de Urgencia N° 006, 2020, artículo 3).

³⁷ Secretaría de Gobierno y Transformación Digital. (2024). *Informe de Opinión Técnica Vinculante N° 001-2024-PCM-SG-SGTD*.

técnica, tener un alcance interinstitucional o multisectorial, y utilizar intensivamente tecnologías digitales o datos.

Finalmente, entre los bloques básicos de interoperabilidad técnica que deben considerarse se encuentran la Plataforma de Interoperabilidad del Estado Peruano (PIDE), la Plataforma de Pagos Digitales (PAGALO.PE), la Plataforma Nacional de Identificación y Autenticación de la Identidad Digital (ID GOB.PE), la Plataforma Casilla Única Electrónica (CASILLA ÚNICA PERÚ), la Plataforma Única de Recepción Documental (MESA DIGITAL PERÚ), la Plataforma Nacional de Software Público (PNSP), la Plataforma Firma Digital (FIRMA PERÚ), y la Infraestructura Tecnológica y Plataforma como Servicio (PaaS) (NUBE PERÚ). Estos bloques proporcionan recursos tecnológicos reutilizables que facilitan la definición, diseño y desarrollo de servicios digitales de manera eficiente y colaborativa.

IV. El derecho a la portabilidad de datos personales ante entidades públicas según el nuevo Reglamento de Protección de Datos Personales

i. Ámbito de aplicación en las entidades públicas

Para nuestra DGTAIPD (2023), la portabilidad de datos permite el derecho de acceso al permitir recibir y transmitir los datos entre diferentes responsables de tratamiento, fomentando a su vez la libre circulación de información y facilitando la transmisión entre distintos proveedores de servicios.

De igual manera, se ha considerado que, “el ejercicio de este derecho tiene sus propias condiciones, como cuando el tratamiento se basa en el consentimiento del individuo o en una relación contractual, así como cuando se realiza mediante medios automatizados” (DGTAIPD, 2023, p. 21). Es por ello que nuestra regulación planteó que no se aplique para el cumplimiento de funciones públicas.

Sin embargo, este planteamiento nos lleva a cuestionar lo siguiente: ¿Cuál debería ser el contenido del presente derecho?³⁸ Si el objetivo es

³⁸ BOLAÑOS, G. (2022). La incorporación del derecho a la portabilidad de datos personales en el ordenamiento jurídico peruano [Tesis para optar el título profesional de Abogado, Universidad de Lima]. Repositorio institucional de la Universidad de Lima. <https://hdl.handle.net/20.500.12724/15999>

garantizar la facultad de control de “reutilización” en entornos digitales que son –plausibles de ser– obtenidos mediante el derecho de acceso. En vista de ello, resulta razonable argumentar que también debiera ser un derecho aplicable a los datos proporcionados de manera directa por el titular incluidos datos observados, brutos respetando derechos de propiedad intelectual y secreto comercial frente a un sujeto privado o una entidad pública. Además, los datos personales vinculados con terceros debieran portar el consentimiento informado de estos cuando corresponda³⁹.

Otro aspecto crucial es el formato de entrega aplicable, que debe ser uno que cumpla con los requisitos de ser estructurado, de uso común y lectura mecánica. Por ello, corresponde la utilización de formatos interoperables con otros sistemas, pero dando los metadatos útiles y esquemas que se tengan disponibles, que precisen el significado de la información intercambiada y permitan la reutilización de los datos con el mejor nivel posible de abstracción sin revelar derechos de terceros⁴⁰. Es decir, tal como el Grupo de Trabajo del Consejo de la Unión Europea, en el glosario del Identificador Europeo de Legislación [ELI] (2019)

³⁹ Al respecto, no debiera hacerse una interpretación excesivamente restrictiva a efectos de permitir portar los datos que también incumban a su titular, pero tomando en cuenta que el nuevo responsable no deberá tratarlos para fines que afecten negativamente derechos y libertades de terceros. Además, resultaría deseable promover la implementación de herramientas que permitan recabar el consentimiento informado, libre, previo expreso e inequívoco de aquellos otros titulares de los datos personales en caso desearan permitir que sus datos personales involucrados sean portados por el solicitante de la portabilidad de sus datos personales.

⁴⁰ No hay recomendaciones específicas sobre los formatos a proporcionar, ya que hay muchos tipos de datos que pueden ser tratados. El formato más adecuado variará entre sectores y “puede que ya existan formatos adecuados que siempre deberían elegirse” para garantizar su interpretabilidad y portabilidad (Grupo de Trabajo, 2017, p. 20). Además, “los formatos que estén sujetos a costosas limitaciones de licencia no deben considerarse una opción adecuada” (p. 20). Se fomenta la “cooperación entre las partes interesadas del sector” para establecer normas y formatos interoperables que satisfagan el derecho a la portabilidad de los datos (Grupo de Trabajo, 2017, p. 20). European Commission. (2017, April 13). *Guidelines on the right to data portability* (WP 242). Article 29 Working Party. https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233

reconoce, un formato que una computadora pueda leer y procesar automáticamente, como es el caso de estos datos comúnmente utilizados CSV, JSON, XML, etc. Además, los datos legibles por máquina deben ser datos estructurados.

Al igual que los demás derechos existentes, el ejercicio del derecho a la portabilidad de datos personales será gratuito siempre y cuando no conlleve una carga técnica excesiva conforme indica el Reglamento (2013, art. 76.2). Para solicitar este derecho, se requieren los nombres y apellidos del titular y su representante (si aplica), una petición concreta de los datos a portar, la dirección electrónica del receptor, y la fecha y firma del solicitante. El proceso debe cumplir con el plazo general y las condiciones previstas en el Reglamento (2013). Además, es fundamental implementar medidas de seguridad como cifrados y protocolos de seguridad, así como una adecuada autenticación tanto del solicitante como del receptor para garantizar la protección de los datos durante la transmisión⁴¹.

Por ello, en adelante se destinarán esfuerzos a determinar si la limitación propuesta al ejercicio de tal derecho frente al sector público resulta acorde con nuestro ordenamiento jurídico y con el contenido constitucional de dicho derecho.

ii. Aplicación de la portabilidad e interoperabilidad para el funcionamiento del sector público

Como se dijo en la introducción, la portabilidad, además de brindar beneficios a los usuarios o titulares de datos personales y que puedan gozar de su derecho a la autodeterminación informativa, es también vista en el marco internacional como un enfoque de política pública para mejorar el acceso e intercambio de datos y su reutilización. Su aplicación va acompañada de medidas análogas o similares que sirven de experiencia y medidas conexas para su fortalecimiento.

⁴¹ Los titulares de datos tienen el derecho a recibir sus datos personales de forma gratuita y sin demoras, así como a transmitirlos entre responsables del tratamiento. Además, los responsables deben informar sobre este derecho, garantizar la seguridad en la transmisión de los datos, proporcionar sólo la información relevante y no retenerla más allá de lo necesario. Estas obligaciones garantizan una portabilidad eficiente y segura, beneficiando a ambas partes.

Para ello, Hoffman y Gonzalez (2020) indican que los principales habilitadores técnicos para lograr la interoperabilidad sintáctica y semántica son la estandarización de datos y las interfaces de programación de aplicaciones o *Application Programing Interfaces (APIs)*⁴². La diferencia clave entre ambos radica en sus implicaciones para la competencia y la innovación. Las *APIs*, diseñadas unilateralmente por el propietario del sistema, producto o servicio, actúan como interfaces de punto final y no requieren un acuerdo de intercambio ni una divulgación completa de información. En contraste, la estandarización de datos, que incluye modelos de datos, formatos y protocolos, requiere un consenso entre las partes involucradas, promoviendo la colaboración y la transparencia en la información (pp. 258).

De momento, se observan diversas formas y mecanismos de ejecución para la portabilidad de datos en el mercado digital, entre ellos:

⁴² Como Hoffmann y Gonzalez (2020) comentan, las *APIs* son herramientas clave para permitir que diferentes sistemas informáticos se comuniquen y compartan datos entre sí. Estas se dividen en “especificaciones”, que definen cómo se debe estructurar la información, y “implementaciones”, que son las instrucciones prácticas para llevar a cabo estas interacciones. Con la llegada de la computación en la nube, los servicios web, que son un tipo de *API*, han ganado mucha importancia, ya que permiten que los sistemas interactúen incluso si están ubicados en diferentes servidores. Aunque los servicios web y las *APIs* tienen muchas similitudes, los servicios web suelen ser más restrictivos en su diseño, mientras que las *APIs* pueden utilizar diferentes métodos de comunicación. Los enfoques más comunes para diseñar *APIs* incluyen SOAP, que se centra en la estructura de la información, y REST, que ofrece una manera más flexible y fácil de usar. También está creciendo en popularidad GraphQL, que permite hacer consultas más específicas para evitar el envío de datos innecesarios. En general, las *APIs* son esenciales para asegurar que los sistemas puedan intercambiar datos de manera efectiva y confiable (pp. 262-262). Hoffmann, J., & Otero, B. (2021). Demystifying the role of data interoperability in the access and sharing debate. *JIPITEC*, 11(3), 252. <https://www.jipitec.eu/archive/issues/jipitec-11-3-2020/5187>

Exportación	Transferencia	Otras soluciones
Los datos se pueden entregar de forma asincrónica (tras un tiempo considerable), por extracción (acceso casi inmediato) o mediante solicitud anticipada (programada para el futuro).	Puede realizarse mediante <i>APIs</i> para un intercambio directo y seguro entre responsables o con terceros que gestionan compatibilidades entre sistemas, garantizando interoperabilidad y reduciendo riesgos (Reimsbach-Kounatze & Molnar, 2024, p. 16) ⁴³ .	Algunas soluciones innovadoras han incluido el uso de herramientas como los PIMS [<i>Personal Information Management Systems</i>], el <i>Data Transfer Project</i> (DTP) iniciado por Google y los <i>Data Trusts</i> , que permiten mejorar la gestión, el control y la transferencia de datos de manera segura y ética.

Fuente: Elaboración propia

Si se considera la portabilidad como un derecho esencial, su implementación debe reflejarse en todos los niveles del sector público y privado. La posibilidad de aplicar mecanismos como la exportación de datos de forma asincrónica o por extracción casi inmediata, así como la transferencia mediante *APIs* o a través de terceros, exige una integración más completa del derecho a la portabilidad.

De acuerdo al Ingeniero Yuri Aldoradin Carbajal (en adelante, “**Ing. Aldoradin**”), especialista en regulación digital en la SGTD, indica que la provisión de servicios públicos a los ciudadanos por vía digital ha sido un gran avance en términos de eficiencia en los últimos años, acelerado por la pandemia del COVID-19. No obstante, muchos de los servicios digitales fueron inicialmente implementados permitiendo la entrega de documentos, incluyendo con ello datos personales a los ciudadanos en formatos comúnmente utilizados, pero que son poco (o no) reutilizables, como el formato “PDF”, lo que limita la capacidad de los usuarios para gestionar y procesar los datos. Así, advierte la poca presencia de formatos reutilizables⁴⁴.

⁴³ REIMSBACH-KOUNATZE, C., & MOLNAR, A. (2024). El impacto de la portabilidad de datos en el empoderamiento de los usuarios, la innovación y la competencia. OECD Going Digital Toolkit Notes, No. 25, OECD Publishing, París.

⁴⁴ “Cuando descargo información, se me da en un PDF, pero si se me diera en otro formato reutilizable, podría gestionar mejor y usarla directamente” (Y. Aldoradin, comunicación personal, 06 de diciembre de 2024).

En la práctica, la normativa peruana contempla mecanismos de portabilidad de datos, permitiendo la transferencia de información personal como parte integral de los servicios a los ciudadanos. Esta evidencia pragmática permite advertir que el derecho a la portabilidad es comúnmente practicado y aplicado por entidades públicas, a pesar de que el Reglamento no lo regule expresamente.

Así, el Ing. Aldoradin destaca que el enfoque más común para diseñar APIs es el SOAP y REST, que provienen del XML. Ello se evidencia en la Plataforma Nacional de Interoperabilidad del Estado Peruano (PIDE), creada y gestionada por la PCM, a través de la SGTD, que será profundizada en el siguiente acápite. Dicha plataforma actúa como un canal intermediario entre los distintos formatos y protocolos del sistema, facilitando el intercambio de datos aunque los sistemas sean técnicamente distintos. Esto garantiza que las entidades públicas puedan consumir y publicar datos sin importar las diferencias en tecnologías o lenguajes utilizados.

De otro lado, aparecen los metadatos⁴⁵ como una opción eficiente para la portabilidad de datos. Como bien indica el Ing. Aldoradin, es importante reconocer la trascendencia y eficacia de los metadatos que permiten optimizar la gestión de la información entre las entidades públicas. No obstante, la realidad es que su uso es mínimo y no se reconoce su alto potencial y utilidad para la portabilidad, inclusive entre el sector público y privado. Dado este escenario, advierte la falta de medidas y políticas en materia de ciberseguridad que permitan la conservación e integridad de los datos personales, lo cual implicaría la utilización del cifrado, sistemas de trazabilidad y doble factor de protección (Y. Aldoradin, comunicación personal, 06 de diciembre de 2024).

En vista de ello, existen indicios de que a la fecha se cuentan con infraestructuras que permiten desarrollar la portabilidad e interoperabilidad en el sector público. Por tanto, a continuación, se analizarán tales productos desarrollados por el Gobierno peruano aplicables a las entidades públicas.

⁴⁵ Según el ISO 23081, se define los metadatos como aquella información estructurada o semiestructurada que permite la creación, gestión y uso de documentos a lo largo del tiempo y dentro de diversos contextos.

A. Plataforma de Interoperabilidad del Estado Peruano (PIDE)

Como se adelantó, la PIDE, a través del uso de APIs, permite la integración y comunicación entre diferentes sistemas gubernamentales, asegurando que la información pueda ser compartida y utilizada de manera coherente a través de diversas plataformas y servicios públicos, lo cual conlleva a una práctica de portabilidad de datos personales. PIDE cuenta con distintos mecanismos de seguridad, como es el caso de autenticación y cifrado de datos, en cuyo caso su aplicación se basa en la Ley No. 27806, Ley de Transparencia y Acceso a la Información Pública y la LPDP junto con su Reglamento.

Así, los “Lineamientos para la suscripción de un Acuerdo de Nivel de Servicio - ANS [Versión 1.0.0]” relativos a la PIDE⁴⁶, reconocen expresamente que toda entidad pública deberá respetar y velar el cumplimiento de la LPDP y su Reglamento. Sobre ello, aunque el uso por parte de las entidades públicas no implica un “almacenamiento de datos”, sí genera la aplicación de la LPDP y su Reglamento conforme al artículo 2.19 de la LPDP⁴⁷. Lo anterior, debido a que el tratamiento de datos personales no requiere que estos sean almacenados, basta con que se lleve a cabo cualquier acción del tratamiento sobre el ciclo de vida de los datos personales, e.g. extraer, consultar, comunicar por transferencia, difundir, u otro tipo de procesamiento que facilite el acceso, correlación o interconexión de los datos personales.

⁴⁶ Secretaría de Gobierno y Transformación Digital (SGTD). Lineamientos para la Suscripción de un Acuerdo de Nivel de Servicio - ANS [Versión 1.0.0] ANS-002-2018. https://cdn.www.gob.pe/uploads/document/file/568956/Lineamientos_ANS_002_2018.PDF?v=1715720937

⁴⁷ Dicho artículo indica lo siguiente: “[E]l tratamiento de los datos personales implica cualquier operación o procedimiento técnico, automatizado o no, que permite la recopilación, registro, organización, almacenamiento, conservación, elaboración, modificación, extracción, consulta, utilización, bloqueo, supresión, comunicación por transferencia o por difusión o cualquier otra forma de procesamiento que facilite el acceso, correlación o interconexión de los datos personales.”

Al respecto, de acuerdo con el “Catálogo Servicios PIDE AGO2024”, publicado por la SGTD (2024)⁴⁸, se determina que existen un total de 1,024 (Un mil veinticuatro) servicios públicos de distintas entidades del Gobierno disponibles en la PIDE, conforme al siguiente estado de disponibilidad asignado:

ACTIVO	206	ACTIVO ALTA de Servicio Web Publicado en PIDE
PROCESO	0	PROCESO de Prueba/Actualización de Servicio Web
BAJA	45	BAJA de Servicio Web segun el proveedor o Norma Legal
PENDIENTE	773	PENDIENTE Ninguna disponibilidad del Servicio Web
TOTAL	1024	

Figura 1

Estado de los servicios web en la PIDE.

Nota. Captura de pantalla del catálogo de servicios de la PIDE contenido en documento excel “Catalogo Servicios PIDE AGO2024”, tomada de la SGTD (2024).

A la fecha, la SGTD (2024) ha informado que, entre enero de 2023 y agosto de 2024, se realizaron 347 millones de transacciones en la PIDE. Esto representó un ahorro de más de S/1 000 millones (Mil Millones con 00/100 Soles) para las instituciones públicas, al evitar el uso de papel y los gastos en notificaciones físicas.

A continuación, y sin perjuicio del estado de disponibilidad vigente, se detallan algunas de las entidades públicas y servicios accesibles a través de la PIDE, conforme al documento Excel “Catálogo de Servicios PIDE AGO2024”. Con ello, tales servicios a su vez podrían implicar el tratamiento de datos personales debido a la naturaleza de datos que se describen en tal catálogo⁴⁹:

⁴⁸ Secretaría de Gobierno y Transformación Digital (SGTD). (2024, 19 de septiembre). *Catálogo de servicios de la PIDE*. [Captura de pantalla]. Presidencia del Consejo de Ministros, Perú. <https://www.gob.pe/institucion/pcm/informes-publicaciones/305761-catalogo-de-servicios-de-la-pide>

⁴⁹ La observación se hace sin perjuicio de que el tratamiento de algunos datos personales mencionados sobre el uso de la PIDE pueda estar exceptuado de la normativa de protección de datos por motivos de seguridad o defensa nacional. Si la normativa es aplicable, el consentimiento para el tratamiento podría estar sujeto a excepciones. Es crucial identificar quién es el responsable del tratamiento en relación con la PIDE. Según la información disponible, la entidad titular de

- **Banco de la Nación [BN]:** “Pago de servicios públicos”, “Servicio de pasarela de pagos en línea”.
- **Ministerio de Salud [MINSA] y Seguro Social de Salud [EsSalud]:** “Consulta de asegurados a EPS por DNI (SUSALUD)”, “Beneficiarios del SIS por DNI”.
- **Ministerio de Trabajo y Promoción del Empleo [MTPE]:** “Consulta de obreros de construcción civil por DNI”, “Registro de contratos de extranjeros por carné de extranjería”, “Consulta de planillas electrónicas de servidores civiles”.
- **Ministerio de Transportes y Comunicaciones [MTC]:** “Consulta de licencias de conducir”, “Consulta de papeletas y sanciones”.
- **Ministerio del Interior [MININTER]:** “Antecedentes Policiales”, “Pensionistas por DNI”, “Consulta sobre órdenes de captura nacional vigentes y no vigentes por apellidos y nombres o DNI”, “Consulta de permiso de lunas polarizadas”, “Consulta de prófugos de la justicia”.
- **Registro Nacional de Identificación y Estado Civil [RENEC]:** “Consulta de DNI (Identificación y Estado Civil)”, “Restricciones en la ficha RENIEC por DNI (fallecido y restricciones generales)”, “Información del padre o madre de la persona por DNI”, “Domicilio Legal y UBIGEO”, “Consulta biométrica de huellas dactilares”, entre otros.
- **Superintendencia Nacional de Migraciones [MIGRACIONES]:** “Consulta de carné PTP”, “Consulta de carné de extranjería”.

Por supuesto, son muchas más las entidades públicas, a nivel nacional, regional y local, que vienen operando a través de la PIDE. Además, también debe tenerse en cuenta que hay varios otros servicios accesibles en tal plataforma que, si bien implican el tratamiento de datos, no necesariamente serán de carácter

cada banco de datos personales que utilice esta herramienta de la SGTD será el responsable, mientras que la SGTD actuaría como encargado del tratamiento. Sin embargo, los bancos de datos generados por cuentas de usuario y datos mínimos necesarios para gestionar accesos en la PIDE podrían calificar como bancos de datos personales de titularidad de la SGTD.

“personal”; y de ser así, no estarían sujetos al régimen de protección de datos personales.

Por ello, estos servicios detallados a modo enunciativo demuestran cómo la PIDE no sólo estandariza y facilita los procesos administrativos en distintos sectores, como el sector salud, sino que también promueve la interoperabilidad entre los sistemas gubernamentales, mejorando la gestión de servicios y la experiencia del usuario en el ámbito público. Al facilitar la integración y el intercambio de información entre diferentes entidades públicas, la PIDE contribuye a una mejor coordinación y mayor eficiencia en la prestación de servicios a la ciudadanía.

En ese contexto, resultan clave los metadatos que, como se ha advertido, proporcionan información sobre otros datos, y su correcta regulación y explotación pueden beneficiar enormemente la portabilidad de datos contribuyendo a una mejor organización, recuperación y uso de la información en sistemas interconectados. Por ello, no deben ser ignorados en la implementación de políticas de portabilidad de datos. Además, como destaca el Ing. Aldoradin, “[l]os metadatos también [pueden calificar como] datos personales que tienen una gran utilidad y no deben ser subestimados” (Y. Aldoradin, comunicación personal, 06 de diciembre de 2024).

B. Concurrencia de entidades públicas en el ejercicio de funcionamiento privado: caso Banco de la Nación (BN)

Un caso particularmente ilustrativo sobre la aplicación del derecho a la portabilidad de datos personales en el ámbito del sector público lo constituye el Banco de la Nación (BN). Esta entidad pública, que cuenta con autonomía económica, financiera y administrativa, no solo desarrolla funciones propias del Estado, sino que también ofrece servicios financieros al público en condiciones comparables a las de los bancos privados. Así, el BN participa de manera activa en el mercado, brindando servicios como cuentas de ahorro, cuentas corrientes, productos de crédito y banca digital a través de canales como su aplicación móvil “App BN”.

Este modelo de funcionamiento plantea interrogantes respecto a la aplicabilidad de la excepción prevista en el artículo 76 del Reglamento de la Ley N.º 29733, que excluye el ejercicio del derecho a la portabilidad cuando el tratamiento de datos es necesario para el cumplimiento de funciones públicas. La pregunta que surge

es si dicha excepción puede aplicarse a los casos en que una entidad pública, como el BN, opera en el mercado en igualdad de condiciones con entidades privadas, ofreciendo servicios bajo esquemas contractuales y voluntarios, y no como parte del ejercicio directo de competencias públicas.

En efecto, los servicios que presta el BN mediante su aplicación digital —como las transferencias inmediatas a otras billeteras digitales (Yape, Plin) o a cuentas de otros bancos— no solo evidencian una dinámica de competencia con el sistema bancario privado, sino que se enmarcan en una política nacional de interoperabilidad liderada por el Banco Central de Reserva del Perú, en cumplimiento del Reglamento de Interoperabilidad de los Servicios de Pago (Circular N.º 0024-2022-BCRP). Esto refuerza la idea de que, en tales escenarios, el BN actúa como proveedor de servicios en condiciones comerciales ordinarias, lo que aleja su actividad de una función pública en sentido estricto.

Por lo tanto, excluir de forma automática el derecho a la portabilidad en estos casos resultaría contradictorio con los principios de igualdad ante la ley y protección de derechos fundamentales, así como con el origen mismo de este derecho, que surge a partir de la experiencia del “open banking” o banca abierta, diseñada justamente para otorgar a los usuarios el control sobre su información financiera y permitirles cambiar de proveedor sin restricciones indebidas.

C. Poder Judicial del Perú [PJ] y Tribunal Constitucional [TC]

En agosto de 2023, el PJ y el TC celebraron convenios específicos de cooperación interinstitucional *“a fin de lograr la interoperabilidad de expedientes y la transferencia de metadatos digitalizados”* (TC, 2023)⁵⁰. Esto se dará en los sistemas que usan cada entidad, Sistema Integrado Judicial [SIJ] del Poder Judicial y Sistema Integrado de Gestión de Expedientes [SIGE] del TC que en una primera etapa sólo se dará en las Cortes Superiores de Justicia.

⁵⁰ Tribunal Constitucional del Perú. (2023). Tribunal Constitucional y Poder Judicial firman convenio de interoperabilidad de expedientes y metadatos digitalizados. <https://www.tc.gob.pe/institucional/notas-de-prensa/tribunal-constitucional-y-poder-judicial-firman-convenio-de-interoperabilidad-de-expedientes-y-metadatos-digitalizados/>

Posteriormente, en una segunda etapa, la interoperabilidad se dará a nivel de Salas Supremas de la Corte Suprema de Justicia, donde el PJ proporcionará los expedientes de la ciudadanía de manera digital al TC, mientras que esta última entidad, le brindará al Poder Judicial el cuadernillo donde se registren todos los actuados en dicha instancia de manera virtual.

El 08 de enero de 2025 la presidenta del TC y la presidenta del PJ se reunieron en razón de los convenios específicos de cooperación firmados a fin de comprometerse para iniciar un plan piloto donde los expedientes digitales puedan transferirse de una institución a otra.⁵¹

D. Sistema de Intermediación Digital (SID)

ELSID-Sunarp es una plataforma que permite iniciar el procedimiento registral mediante la creación del parte notarial electrónico, la incorporación de la firma digital del notario y su envío al domicilio electrónico de la Superintendencia Nacional de los Registros Públicos [SUNARP]. Este sistema requiere la colaboración del ciudadano, el notario y el registrador público para su correcta operatividad.

Al respecto, el Notario Fredy Otárola Peñaranda (en adelante, **Dr. Otárola**) advierte que, si bien es un sistema diseñado para la celeridad de los trámites notariales, este presenta importantes limitaciones técnicas y jurídicas que afectan el acceso, interoperabilidad y reutilización de los datos registrados (F. Otárola, comunicación personal, 07 de diciembre de 2024). Un aspecto fundamental es la utilización de documentación, en su mayoría, en formato PDF, lo cual dificulta su procesamiento automático y la extracción de información estructurada. A diferencia de los formatos abiertos y legibles por máquina, los archivos PDF no permiten acceder a los datos de manera granular ni procesarlos mediante sistemas automatizados, lo que genera ineficiencia en el manejo de grandes volúmenes de información. Además, el uso de PDF impide la integración efectiva de la información con otras

⁵¹ Tribunal Constitucional del Perú [@TC_Peru]. (2025, enero 08 <https://x.com/tc-peru/status/1877035658725732816?s=46&t=LP-Zj-25DdPYyBdrO5u-Qg>)

bases de datos públicas y privadas, limitando las posibilidades de interoperabilidad que serían clave para el desarrollo de servicios digitales más avanzados.

A partir de las declaraciones del Dr. Otárola, advertimos nuevamente la falta de acceso a los metadatos asociados a los documentos registrados dentro del SID-SUNARP. Sin metadatos accesibles, las entidades públicas, los ciudadanos y las empresas tienen dificultades para localizar y utilizar la información registrada de manera eficiente, lo que genera retrasos y costos adicionales en los procesos administrativos.

Por otro lado, el carácter de documento con función pública atribuido al instrumento notarial constituye una restricción jurídica relevante que limita la reutilización de los datos registrados en los sistemas digitales. En el marco normativo peruano, los documentos notariales se encuentran dotados de fe pública, lo que les otorga un carácter solemne e inmutable. Esto implica que la información contenida en dichos documentos no puede ser modificada, fragmentada ni utilizada con un propósito distinto al que originalmente motivó su creación. Esta naturaleza inalterable del documento notarial representa un obstáculo para el aprovechamiento de los datos contenidos en los registros, impidiendo que dicha información sea utilizada para otros fines de utilidad.

En ese sentido, los datos registrados en el SID-SUNARP permanecen encapsulados en formatos rígidos y estáticos, limitando su reutilización y dificultando la creación de ecosistemas de datos abiertos que puedan ser aprovechados por entidades públicas o privadas para impulsar la innovación digital en los servicios registrales.

En definitiva, el SID-SUNARP ha representado un avance digital interesante para el ecosistema notarial. No obstante, se ha dejado de lado la posibilidad de la reutilización de la información alojada en tal sistema, incluyendo los metadatos de distinta naturaleza a nivel notarial y registral, cuando estos podrían aprovecharse de sobremanera y fomentar la generación de usos y mercados derivados tanto en cabeza del propio titular de los datos personales, como por parte de terceros que éste autorizará, conforme se dicta en el Reglamento en cuanto al derecho a la portabilidad.

Con todos los casos analizados, es evidente la existencia de la portabilidad *de facto* en torno a los datos personales, la cual se viene ejerciendo mediante el uso de los servicios digitales mencionados, especialmente en el marco de la PIDE y los bloques de interoperabilidad del Estado Peruano. Esto ocurre principalmente para el ejercicio de las competencias conferidas a las entidades públicas y con el fin de brindar servicios a los ciudadanos que lo requieren. Como se evidencia, dicho derecho ya se está ejerciendo *de facto* a solicitud de los ciudadanos para la provisión de servicios digitales en el marco de las competencias de cada entidad pública, gracias a los grados de interoperabilidad implementados en el Gobierno entre las entidades públicas.

Este panorama nos lleva a otra interrogante: ¿cómo puede extenderse y materializarse tal derecho en armonía con el ejercicio de las competencias de las entidades públicas, frente al sector público y los propios ciudadanos, titulares de los datos personales? Como se ha detallado, las entidades públicas solo deberían realizar un tratamiento de datos personales acorde con las competencias legalmente previstas, lo cual está contemplado de manera uniforme para todos los derechos existentes en la normativa de protección de datos personales.

Por ello, se recomienda destinar esfuerzos a materializar la posibilidad de reutilización de datos personales por parte del propio ciudadano, permitiéndole que sea técnicamente viable transferir sus datos personales y demás información obtenida en el marco de los servicios digitales a otros responsables del sector privado. Algunas experiencias comparadas y tendencias a nivel global, que serán estudiadas en la siguiente sección, muestran que la implementación de mecanismos que combinen la posibilidad de portar datos personales y otra información obtenida a través de los servicios digitales proporcionados a los ciudadanos podría contribuir a mejorar el bienestar social y económico de la población.

iii. Portabilidad en las competencias públicas a nivel internacional

En el ámbito internacional, diversos países han implementado iniciativas que permiten a los ciudadanos gestionar sus datos personales de forma segura y accesible, reconociendo el constante flujo de información entre entidades públicas. Por ejemplo, India ha desarrollado **DigiLocker**,

una plataforma digital donde los ciudadanos almacenan documentos oficiales. En Latinoamérica, **Brasil** cuenta con el portal **Gov.br** y **Colombia** con la **Carpeta Ciudadana Digital**, ambos orientados al acceso centralizado de servicios públicos y documentos digitales.

Además, herramientas como los **sandboxes regulatorios**, el **Data Transfer Project (DTP)** y los **data trusts** se perfilan como soluciones clave para fortalecer el derecho a la portabilidad de datos. En particular, los *data trusts* son modelos fiduciarios que gestionan datos personales de forma ética y transparente, protegiendo los intereses de los titulares.

Casos concretos como el **NHS Data Trust en Reino Unido** y **MIDATA en Suiza** demuestran cómo estos mecanismos pueden facilitar el intercambio de datos en tiempo real para mejorar servicios de salud e investigación, garantizando siempre el consentimiento informado y la protección de la privacidad. Estos ejemplos evidencian la necesidad de adaptar los marcos normativos locales para incluir a las entidades públicas y promover una portabilidad de datos efectiva y equitativa.

VI. Conclusiones

- La portabilidad y la interoperabilidad son esenciales en la gestión de datos digitales. La portabilidad permite transferir datos entre sistemas sin reingresarlos, usando formatos comunes para facilitar su reutilización. La interoperabilidad, en cambio, asegura que diferentes sistemas puedan intercambiar y utilizar la información de manera efectiva. Mientras la portabilidad se enfoca en el movimiento de datos, la interoperabilidad garantiza su comprensión y uso adecuado. Ambos conceptos están interrelacionados y son cruciales para la eficiencia y conectividad digital. Su éxito depende de la colaboración entre actores (privados y públicos), y su implementación conlleva riesgos de seguridad y confidencialidad que deben ser gestionados con cuidado para prevenir brechas y asegurar una protección adecuada.
- El derecho a la autodeterminación informativa incluye la capacidad de obtener y usar información personal, pero la normativa actual, como el Reglamento (2013), limita la reutilización efectiva de los datos debido a formatos no reutilizables. Así, este derecho emerge como una extensión necesaria del derecho de acceso, adaptándose a la digitalización y superando las limitaciones actuales.

- La portabilidad de datos constituye un derecho fundamental para garantizar el control del titular sobre su información personal y promover la interoperabilidad en entornos digitales, facilitando el intercambio seguro y reutilización de datos entre distintas entidades. No obstante, limitar su aplicación frente al sector público reduce su potencial transformador, ya que excluye datos que podrían optimizar servicios y mejorar la transparencia administrativa. Por ello, resulta esencial avanzar hacia una interpretación más amplia que considere también los datos observados, derivados e inferidos, utilizando formatos estructurados y legibles por máquina, acompañados de metadatos útiles que permitan su reutilización eficiente, respetando derechos de terceros y garantizando medidas de seguridad adecuadas. Así, la portabilidad de datos se consolida como una herramienta clave para fortalecer la autonomía digital, impulsar la innovación y mejorar tanto los servicios públicos como privados en beneficio de la sociedad.
- El utilizar solo formatos no reutilizables, como los archivos PDF, limitan la portabilidad de datos y su aprovechamiento por los ciudadanos, así como de otras entidades públicas. Si bien existen mecanismos de interoperabilidad, como la Plataforma PIDE, que facilita el intercambio de información entre entidades públicas, su efectividad depende del uso de formatos estructurados y metadatos que optimicen la gestión de los datos. Sin embargo, el uso de metadatos sigue siendo limitado, y las medidas de ciberseguridad necesarias para garantizar la protección e integridad de los datos personales aún son insuficientes. Por ello, resulta esencial fortalecer las políticas públicas que promuevan la reutilización segura de los datos y adopten tecnologías de portabilidad avanzadas, asegurando una gestión de información más eficiente y segura en beneficio de los ciudadanos.
- La experiencia internacional y local demuestra que tanto la estandarización de datos como el uso de *APIs* son esenciales para lograr una interoperabilidad efectiva. Mientras que las *APIs* permiten una transferencia continua y en tiempo real de datos, los sistemas de estandarización promueven la transparencia y la colaboración. Ambos aspectos son esenciales para un ecosistema en el que se busca garantizar la facultad de reutilizar la información, sobre todo si es de carácter personal.

- El Reglamento propone que el derecho a la portabilidad no sea aplicable a entidades públicas que traten datos en el ejercicio de sus funciones. De entrada, ello podría indicar que la portabilidad de datos sí deba aplicarse a aquellos datos personales que sean tratados por entidades públicas con base en cualquier otra finalidad adicional que no esté estrechamente vinculada con el ejercicio de sus funciones y que por ende requieran del consentimiento de los ciudadanos.
- No obstante, el pretender limitar este derecho únicamente a entidades privadas no sería acorde con las limitaciones propuestas a todos los demás derechos. Tal limitación no se encuentra en ninguno de los otros derechos de la LPDP ni a nivel constitucional. Inclusive, el derecho de acceso, estrechamente vinculado a la portabilidad, no presenta tal restricción frente a la Administración Pública.
- La esencia de los derechos fundamentales y bienes jurídicos a proteger trasciende el marco normativo o reglamentario que engloba su protección. La implementación práctica y la existencia de mecanismos de portabilidad e interoperabilidad a nivel del Estado peruano, especialmente dentro del marco del Sistema Nacional de Transformación Digital, demuestran que la portabilidad de datos personales ya se está llevando a cabo *de facto* en la prestación de diversos servicios digitales públicos a nivel nacional. Por lo tanto, resulta inexacto afirmar que este derecho no se está aplicando en el ejercicio de las competencias de las entidades públicas únicamente porque el régimen reglamentario propuesto lo sugiera. En realidad, al considerar la situación de manera integral e interpretativa, parece que este derecho ya se está implementando de acuerdo con la naturaleza y necesidades de las competencias y los servicios proporcionados por cada entidad pública.
- En vista de ello, el derecho a la portabilidad de datos personales debería ser aplicable y exigible ante las entidades públicas peruanas considerando las particularidades del caso. Para ello:
 - a. Debe seguirse el marco del ámbito de aplicación previsto en la LPDP, respetando las mismas excepciones y limitaciones que se aplican a los otros derechos de los titulares de datos personales existentes, junto con otras que puedan surgir durante la implementación de este derecho.
 - b. El reto es materializar este derecho de forma efectiva, equi-

librando las competencias de las entidades públicas con la facultad de los ciudadanos para disponer de sus propios datos. Para ello, es necesario promover formatos y mecanismos que faciliten la reutilización de los datos personales y otra información obtenida a través de los servicios digitales, ya sea por los ciudadanos o por otros responsables del sector privado que ellos autoricen.

- c. Aunque la portabilidad de datos personales ya se ejerce *de facto* en Perú a través de la PIDE y la interoperabilidad de las entidades públicas para el ejercicio concreto de sus facultades o competencias, aún falta explorar el potencial de reutilizar la información almacenada, incluidos los metadatos, frente a los ciudadanos. Esta reutilización podría generar nuevos usos y mercados, beneficiando tanto a los titulares de los datos como a terceros autorizados, conforme al derecho a la portabilidad.
 - d. Las experiencias internacionales muestran que habilitar la portabilidad y reutilización de datos puede mejorar el bienestar social y económico, fomentando la innovación y la creación de nuevos mercados. Esto permitirá a los ciudadanos ejercer plenamente su derecho a la portabilidad y generar beneficios tanto para ellos como para la sociedad en general. Este enfoque, respaldado por la interoperabilidad estatal, promueve la innovación y garantiza el control ciudadano sobre sus datos.
- Sin duda, a nivel local sigue pendiente el explorar cómo la portabilidad de datos no solo puede mejorar la eficiencia dentro del sector público, sino también promover una mayor integración entre los sectores público y privado. En sectores como salud, educación o transporte, la transferencia de datos personales de forma segura podría generar mejoras en el servicio y la atención al usuario. Muchos son los ejemplos en los cuales vienen configurándose una portabilidad de datos personales *de facto* entre distintas entidades del sector público para la provisión de servicios públicos solicitados por ciudadanos peruanos. Hoy más que nunca, en un país interconectado donde la PIDE y los distintos bloques de interoperabilidad componen los pilares de las plataformas transversales en todos los niveles de gobierno, el Estado peruano debe abrazar la portabilidad desde el diseño de la mano de las facultades de control de los titulares de datos personales peruanos.

Más allá del reciente cambio de opinión de la Administración Tributaria, ¿cuál es la forma correcta de calificar un servicio como digital para fines del Impuesto a la Renta?

Sussel Xiomara Landeo Huamán*

Resumen.- Este artículo analiza el tratamiento tributario de los servicios digitales en el Perú, centrado en la interpretación del listado del Reglamento del Impuesto a la Renta. Se sostiene que un servicio solo califica como digital si cumple con los requisitos esenciales previstos en la norma. En este sentido, se busca reflexionar sobre la forma correcta de leer dicho listado sin perjuicio del reciente cambio de opinión de la Administración Tributaria mediante el Informe No. 046-2025-SUNAT/7T0000.

Palabras claves.- Servicios digitales – Impuesto a la Renta – Comercio electrónico.

Abstract.- This article analyzes the tax treatment of digital services in Peru, focusing on the interpretation of the list contained in the Income Tax Regulations. It argues that a service qualifies as digital only if it meets the essential requirements established by law. In this regard, the article seeks to reflect on the proper way to construct said list, notwithstanding the recent change in the Tax Administration's position as set forth in Report No. 046-2025-SUNAT/7T0000.

Keywords.- Digital services – Income Tax – Peruvian Tax Administration, E-commerce.

* Abogada senior del área de Consultoría Tributaria en EY Perú con más de 6 años de experiencia en consultoría tributaria para empresas nacionales e internacionales. Realizó un Summer Course en International Tax Law en ITC Leiden, Singapur, y un PEE en Derecho Empresarial y Financiero en ESAN. Miembro activo del IPDT, GES- UNMSM y CAL, es autora de artículos tributarios y conferencista en foros académicos.

I. Regulación de los servicios digitales en la Ley del Impuesto a la Renta y su Reglamento

La vigente Ley del Impuesto a la Renta (en adelante, la “Ley del IR”) establece que los sujetos no domiciliados en el país tributan vía retención por sus rentas de fuente peruana¹.

A su vez, el artículo 9 de la Ley del IR establece los supuestos de renta de fuente peruana, siendo uno de ellos el de actividades civiles, comerciales, empresariales o de cualquier índole, que se lleven a cabo en territorio nacional, cuya tasa de retención es del 30%². Siguiendo una interpretación contraria de esta norma, las de actividades civiles, comerciales, empresariales o de cualquier índole, esto es, los servicios en general, que no se lleven a cabo en territorio peruano no se encuentran sujetos a retención del Impuesto a la Renta (en adelante, “IR”) en Perú.

La excepción a esta regla son los servicios de asistencia técnica y digitales utilizados económicamente en el país, los cuales, sin importar el lugar en que se presten, se encuentran sujetos a retención del IR con las tasas del 15% y 30%, respectivamente³.

Dado que el objetivo de este trabajo es abordar los servicios digitales utilizados económicamente en el Perú. A continuación, comentaremos su regulación en la Ley del IR y su Reglamento.

i. Ley del IR

Los servicios digitales fueron introducidos en la Ley del IR en el 2004 mediante el Decreto Legislativo 945, el cual incorporó el inciso i) del artículo 9⁴.

Posteriormente, mediante el Decreto Legislativo 970 -vigente desde el

¹ Artículos 6, 71 y 76 de la Ley del IR.

² Según el inciso e) del artículo 9 de la Ley del IR y el artículo 56 de esta misma Ley.

³ Según el artículo 56 de la Ley del IR.

⁴ Cuyo texto era el siguiente:

Artículo 9.-En general y cualquiera sea la nacionalidad o domicilio de las partes que intervengan en las operaciones y el lugar de celebración o cumplimiento de los contratos, se considera rentas de fuente peruana:

(...) Las obtenidas por servicios digitales prestados a través del Internet, cuando el servicio se utilice económicamente, use o consuma en el país.

año 2007 y cuyo texto continúa vigente hasta hoy-, se sustituyó el referido inciso i) del artículo 9º de la Ley del IR para incluir redes equivalentes al internet, manteniendo como criterio esencial la utilización económica del servicio en el país⁶.

Según la Exposición de Motivos del Decreto Legislativo Nro. 945, los servicios digitales regulados en nuestra legislación pertenecen al género “E-commerce”. En efecto, este género comprende a las ventas de bienes tangibles, prestación de servicios⁷ y operaciones con intangibles.

Así, aun cuando el “E-commerce” comprende otras operaciones, el legislador se limitó a gravar con el IR únicamente los servicios digitales.

La razón de ello fue que el legislador buscó cubrir rentas antes no sujetas a imposición por ausencia de criterios de conexión aplicables, introduciendo nuevas reglas de fuente basadas en el lugar de uso, consumo o aprovechamiento económico del servicio, pero no definió con precisión qué características convierten a un servicio en “digital”.

⁵ Cuyo texto es el siguiente:

Artículo 9.- En general y cualquiera sea la nacionalidad o domicilio de las partes que intervengan en las operaciones y el lugar de celebración o cumplimiento de los contratos, se considera rentas de fuente peruana:

(...) Las obtenidas por servicios digitales prestados a través del Internet o de cualquier adaptación o aplicación de los protocolos, plataformas o de la tecnología utilizada por Internet o cualquier otra red a través de la que se presten servicios equivalentes, cuando el servicio se utilice económicamente, use o consuma en el país.

⁶ Nótese que, que los alcances de servicios digitales introducidos mediante el Decreto Legislativo 945, no fueron modificados con el Decreto Legislativo 970, puesto que este solo precisó las redes equivalentes al internet.

⁷ Servicios calificados como digitales según la Exposición de Motivos del Decreto Legislativo Nro. 945:

- Mantenimiento de software: Contratos de mantenimiento de software usualmente ofrecen actualizaciones del software adquirido y servicio técnico. Si los cargos por cada concepto (las actualizaciones y el servicio técnico) se realizan de forma separada, el tratamiento puede diferenciarse en ese sentido. Si los cargos no se separan la transacción en su totalidad será tratada como venta de bienes.
- Soporte técnico al cliente en red: El vendedor provee al consumidor de un servicio que se presta a través de la misma red. El servicio puede comprender

Desde nuestro punto de vista, este criterio expuesto en el último párrafo resulta de suma relevancia para los fines del presente ensayo, dado que la Ley del IR se limitó a señalar que califican como servicios digitales los prestados a través de Internet que sean utilizados económicamente en el país no determinando qué características deben de cumplir los servicios prestados mediante Internet para calificar como digitales.

Como veremos en el punto siguiente, dichas características fueron reguladas en el Reglamento de la Ley del IR, en el cual también se incorporó el listado de servicios que califican como digitales que inicialmente había formado parte de la Exposición de Motivos de la Ley del IR.

recomendaciones de instalación, la provisión de documentación técnica, bases de datos o conexión automática a través del correo electrónico con personal técnico.

- Data Warehousing: El cliente almacena su información computarizada en los servidores de propiedad del prestador del servicio los que son operados por éste. El cliente puede acceder, almacenar y manipular tal información de manera remota.
- Application hosting: El cliente almacena su información computarizada en los servidores de propiedad del prestador del servicio los que son operados por éste. El cliente puede acceder, almacenar y manipular tal información de manera remota.
- Provisión de servicios de aplicación: El prestador del servicio de aplicación (ASP) pone a disposición del cliente una aplicación de software almacenada en servidores de su propiedad y controlados por él. El manejo del software por parte del cliente es equivalente a una situación en la que el cliente tuviera contratados servicios de outsourcing mediante los cuales una oficina remota una vez accesado al software, puede ordenar, pagar y obtener bienes o servicios ofrecidos por terceras partes, desde equipo de oficina hasta reservaciones aéreas para los ejecutivos.
- Almacenamiento de páginas de Internet (web site hosting): El proveedor ofrece espacio en su servidor para almacenar páginas o sitios web no obteniendo ningún derecho sobre el contenido de la página cuando ésta es insertada en el servicio de su propiedad. El proveedor es compensado con un honorario fijado en función a la duración del contrato.
- Acceso electrónico a servicios de consultorio: Comprende los servicios de consultores, abogados, médicos u otros, profesionales que provean de senados profesionales a través del correo electrónico, video teleconferencia u otro medio remoto de comunicación.
- Propaganda y publicidad: Propagandistas pagan por tener diseminado en

ii. Reglamento de la Ley del IR

En el 2004, el Decreto Supremo 086-2004-EF incorporó al Reglamento de la Ley del IR las características y el listado de servicios calificados como digitales.

Se definió al servicio digital como aquel puesto a disposición del usuario a través de Internet u otra red similar mediante acceso en línea, que es esencialmente automático y no viable sin tecnología de la información. Así, se incluyeron como supuestos de servicios digitales al mantenimiento de software, soporte técnico en línea, almacenamiento de información, hospedaje de aplicaciones, servicios ASP, web hosting, consultoría electrónica, publicidad digital, subastas en línea, distribución electrónica de información, acceso a páginas interactivas, capacitación remota y portales de compraventa.

determinadas páginas o sitios web sus avisos de publicidad. Estos avisos son pequeñas imágenes gráficas contenidas en un sitio de la red. Las tasas que se fijan varían desde el número de veces en que el aviso es mostrado al potencial cliente hasta el número de veces en que un cliente ingresa al aviso desplegado en la página web.

- Remate en línea: El proveedor de Internet oferta diversos ítems para que sean adquiridos por remate. El usuario adquiere los bienes directamente del propietario de tales bienes. El vendedor compensa al proveedor de Internet con un porcentaje de la venta.
- Reparto de información: El proveedor de internet distribuye electrónicamente Información a los suscriptores en función de sus preferencias personales. El principal valor para los clientes es la conveniencia de recibir información en formato reducido diseñada según sus específicas necesidades.
- Acceso a una página o sitio interactivo de Internet: El proveedor pone a disposición de los suscriptores una página web caracterizada por su contenido digital (información, música, videos, juegos). Los suscriptores pagan una comisión fija por el acceso al sitio o página. El principal valor del sitio de Internet para los suscriptores es su interacción con la página más que la posibilidad de conseguir el producto o el servicio de la red.
- Portales en línea para la contraventa: El operador de una página de internet almacena en sus servidores de bienes o servicios. Los usuarios de tales sitios de Internet pueden seleccionar productos de estos catálogos y efectuar órdenes en línea. El operador de internet transmite sus órdenes a los proveedores quienes son responsables de aceptar y dar trámite a las órdenes. Los proveedores pagan una comisión al operador del sitio equivalente a un porcentaje de las órdenes realizadas.

Posteriormente, el Decreto Supremo 159-2007-EF precisó que dichos servicios también podían prestarse a través de redes similares al Internet, sin alterar sus características esenciales. Actualmente, esta definición se recoge en el inciso b) del artículo 4-A del Reglamento, estableciendo un marco normativo que delimita con mayor claridad el universo de servicios digitales sujetos a imposición en el Perú.

Como se puede observar, los primeros párrafos del inciso b) del artículo 4-A del Reglamento de la Ley del IR brindan mayores alcances de lo que debe entenderse por servicios digitales. Así, es posible resaltar los siguientes aspectos:

- El primer párrafo regula las características esenciales o requisitos necesarios que deben cumplir los servicios para calificar como digitales. Estas características –que serán comentadas a mayor detalle en el punto siguiente– son (i) que exista un servicio, (ii) que se preste a través de Internet o una red similar, (iii) que requiera de acceso en línea, (iv) que sea esencialmente automático, y (v) que no sea viable en ausencia de la tecnología de la información.
- El segundo párrafo establece un listado no taxativo de trece servicios que califican como digitales.

Ahora bien, para identificar por qué se regularon determinadas características como esenciales para que un servicio califique como digital y porqué además se reguló un listado de servicios que califican como digitales, corresponde remitirnos a la Exposición de Motivos del Decreto Supremo 086-2004-EF.

Al respecto, la definición de servicio digital y requisitos mínimos que deben cumplirse para calificar como tal provino del documento de trabajo denominado “TAXUD 2303/03 Rev 2 final - VALUE ADDED TAX COMMITTEE” de la Comisión Europea⁸.

⁸ Sobre la definición y características que deben cumplir los servicios digitales, la Exposición de Motivos del Decreto Legislativo 945 señala lo siguiente: “Como quedó sustentado en la exposición de motivos del Decreto legislativo N° 945, los servicios digitales son una especie de los productos digitales (que incluyen a los bienes digitales y a las transacciones con intangibles) que se caracterizan, básicamente, por transferirse en línea a los usuarios a través de la técnica de la descarga electrónica (download). Para definir a los servicios digitales se han considerado, además de la característica antes enunciada, algunos aspectos del

Desde nuestra perspectiva, es importante realizar un contraste de los requisitos que deben cumplir los servicios digitales según el referido documento de la Comisión Europea con el texto recogido en el Reglamento de la Ley del IR:

Requisitos que deben cumplir los servicios digitales según la Comisión Europea	Requisitos que deben cumplir los servicios digitales según el Reglamento de la Ley del IR
1) Es entregado mediante Internet o una red electrónica (basada en internet o redes similares). 2) La naturaleza del servicio es altamente dependiente de la tecnología de la Información para su suministro: ▪ El servicio es esencialmente automático. ▪ Involucra una mínima intervención humana. ▪ No es viable en ausencia de la tecnología de la Información.	▪ Es un servicio. ▪ Se presta a través de Internet: O cualquier otra red similar (intranet y extranet). ▪ Requiere acceso en línea ▪ Es esencialmente automático. ▪ No debe ser viable en ausencia de la tecnología de la información.

Lo anterior confirma que el documento emitido por la Comisión Europea fue una referencia fundamental para regular la definición y características de los servicios digitales en el Reglamento de la Ley del IR. Asimismo, permite identificar que el requisito de automaticidad del servicio está vinculado a la exigencia de una mínima intervención humana en su prestación.

concepto de ‘servicio prestado por vía electrónica’ que ha definido el Comité del Impuesto al Valor añadido de la Comisión Europea en el documento de trabajo TAXUD 2303/03 Rev 2 final - VALUE ADDED TAX COMMITTEE (Article 29 of Directive 77/388/EEC (Bruselas, 2003), encargada de evaluar la aplicación de las normas comunitarias del IVA en relación a las operaciones de comercio electrónico. Así, para el referido Comité un ‘servicio prestado por vía electrónica’ es aquel que guarda los siguientes elementos: (i) es aquel que es entregado a través de Internet u otra red electrónica; (ii) la naturaleza del servicio es altamente dependiente en las tecnologías de información; y, (iii) **requiere una mínima intervención humana.**” (Énfasis agregado).

Cabe señalar, además, que el documento emitido por la Comisión Europea incluye un listado de servicios susceptibles de ser calificados como digitales y otro de aquellos que, por sus características, no cumplen con dicha calificación. A continuación, se presenta parte de este listado:

A. Servicios calificados como digitales

Concepto	Ejemplos
Suministro de sitios web, alojamiento web y mantenimiento a distancia de programas y equipos	Mantenimiento a distancia automatizado y en línea de los programas
	Alojamiento de sitios y páginas web
	Administración remota de sistemas
	Almacenamiento de datos en línea (es decir, donde los datos específicos se almacenan y recuperan electrónicamente)
	Suministro en línea de espacio en disco a la carta
Enseñanza a distancia	Enseñanza automatizada y dependiente de Internet o de una red electrónica similar para funcionar, incluidas las aulas virtuales.
	Cuadernos de trabajo completados por el alumno en línea y calificados automáticamente, sin intervención humana.

B. Servicios no calificados como digitales

Concepto	Razonamiento
Servicios de abogados y consultores financieros, etc., que asesoran a los clientes a través del correo electrónico	Esta es una prestación de servicios que depende de una intervención humana sustancial y el Internet o la red electrónica solo se utiliza como medio de comunicación
Servicios de enseñanza interactiva en los que el contenido del curso es impartido por un profesor a través de Internet o de una red electrónica (es decir, a través de un enlace remoto)	

De lo anterior se tiene que el documento en el cual se basó el Reglamento de la Ley del IR expresamente **excluye a los servicios que dependen de una intervención humana sustancial como digitales, debido a que no cumplen con el requisito de ser esencialmente automáticos.**

La Exposición de Motivos del Reglamento de la Ley del IR aclara que el listado de servicios digitales incorporado en la norma tiene carácter no taxativo. Además, señala como fuentes de referencia dos documentos clave a nivel internacional: (i) el Reporte Final de la OCDE sobre caracterización de rentas vinculadas al comercio electrónico, y (ii) el documento de trabajo de la OCDE titulado “¿Son actuales reglas de los convenios para evitar la doble imposición apropiadas para gravar los beneficios empresariales provenientes del comercio electrónico?”. Esta referencia internacional subraya la intención del legislador de alinear el marco tributario peruano con estándares globales, aunque deja abierta la necesidad de precisar criterios sustantivos para delimitar el alcance del concepto de servicio digital.

Al respecto, debemos señalar que el primero de dichos documentos contiene un listado de 29 operaciones de comercio electrónico, siendo que algunas de ellas guardan similitud con el listado regulado en el Reglamento de Ley del IR. Por su parte, el segundo documento contiene operaciones mucho más generales de comercio electrónico (que no es servicio digital propiamente dicho según lo expuesto líneas arriba).

De lo anterior se tiene que la definición y requisitos necesarios de los servicios digitales se basó en un documento emitido por la Comisión Europea; mientras que el listado de trece operaciones que califican como digitales se basó en documentos emitidos por la OCDE.

A continuación, presentamos un resumen de los aspectos más resaltantes de ambos documentos (ver siguiente página).

De lo expuesto en este punto es posible concluir que la Ley del IR regula el supuesto de hecho que configura renta de fuente peruana sujeta a retención en Perú y su criterio de conexión: Servicios digitales prestados a través de Internet o alguna otra red similar que sean utilizados económicamente, usados o consumidos en el Perú.

No obstante, no brinda mayor alcance sobre qué debe entenderse por servicio digital, para lo cual es preciso remitirse al Reglamento de la Ley del IR, el cual consta de dos partes:

- a. Una primera parte en la que se regulan los cinco requisitos necesarios para que un servicio digital califique como tal.
- b. Un listado no taxativo de trece operaciones que califican como digitales.

Comité del Impuesto al Valor añadido de la Comisión Europea	Documento de trabajo de la OCDE
• Establece los requisitos esenciales para que el servicio sea calificado como digital, entre ellos, ser esencialmente automático. • Establece un listado de operaciones que califican como servicios digitales, en el que se evidencia que son esencialmente automáticos. • Establece un listado de operaciones que no califican como servicios digitales en donde se encuentra los servicios de abogados y consultores financieros mediante correo electrónico y cuya razón de su exclusión es que requieran una sustancial intervención humana y son viables mediante otros medios de comunicación.	• No define a los servicios digitales ni establece sus características ni requisitos esenciales. • Establece operaciones de <i>E-commerce</i> (comercio electrónico), las cuales deben ser categorizadas. Incluye la prestación de servicios y otras operaciones de comercio electrónico como venta de software, mantenimiento de software, y otras en el contexto del comercio electrónico, pero que no son esencialmente automáticos. • Aun cuando no define al servicio digital, se recogieron estos supuestos para elaborar el listado del Reglamento de la Ley del IR.

En el punto siguiente explicaremos que la forma en que ambas partes deben ser leídas admite más de una interpretación, siendo que el punto subsiguiente desarrollaremos los argumentos que sustentan cada una de ellas.

II. Problemática: Ambigüedad interpretativa y posibles interpretaciones

Según se explicará en este punto, existe más de una forma de leer el primer y segundo párrafo del inciso b) del Artículo 4-A del Reglamento de la Ley del IR.

De una lectura conjunta es posible evidenciar una incongruencia entre ambos párrafos, puesto que el primero establece requisitos generales que deben cumplir los servicios para calificar como digitales, mientras que el segundo contiene un listado de servicios que califican como tales aun cuando de su texto se evidencia que no cumplen con el íntegro de los requisitos generales previstos en el primer párrafo.

Al respecto, el primer párrafo del Reglamento de la Ley del IR establece los requisitos que deben de cumplir los servicios digitales para calificar como tales, siendo estos los siguientes:

- Que exista un servicio. Esto es, una prestación realizada por un proveedor a un cliente.
- Que se preste a través de Internet, o cualquier otra red similar (intranet y extranet).
- **Requiere acceso en línea. Esto es, que se debe estar conectado a la red para recibir una respuesta automática.**
- Que sea esencialmente automático, lo cual, según el documento emitido por la Comisión Europea que motivó esta regulación, debe ser viable con mínima o incluso nula intervención humana.
- No debe ser viable en ausencia de la tecnología de la información, lo que implica que requiere un desarrollo mínimo de herramientas informáticas.

Queda claro que estos requisitos legales son concurrentes en tanto forman parte de un mismo párrafo, de modo que, si un servicio no cumple con alguno de ellos, este no podrá ser calificado como servicio digital.

Por su parte, el segundo párrafo del Reglamento de la Ley del IR establece un listado taxativo de servicios que califican como digitales, siendo relevante resaltar los contenidos en los numerales 2 y 7 del inciso b) del artículo 4-A⁹ de esta norma porque claramente no cumplen con el requisito de ser esencialmente automáticos y requieren de una importante intervención humana.

Siendo ello así, es posible advertir una clara contradicción entre el primer y el segundo párrafo de la norma analizada, puesto que el primero exige como requisito necesario para que un servicio califique como digital el que el servicio sea esencialmente automático, esto es, que cuenten con una mínima intervención humana; mientras que el segundo establece que califican como servicios digitales servicios que no cumplen con ser esencialmente automáticos (en tanto cuentan con una preponderante intervención humana).

⁹ Artículo 4-A. - "(...) 2. Soporte técnico al cliente en red: Servicio que provee soporte técnico en línea incluyendo recomendaciones de instalación, provisión en línea de documentación técnica, acceso a base de datos de solución de problemas o conexión automática con personal técnico a través del correo electrónico (...) 7. Acceso electrónico a servicios de consultoría: Servicio por el cual se pueden proveer servicios profesionales (consultores, abogados, médicos, etc.) a través del correo electrónico, video conferencia u otro medio remoto de comunicación."

Para superar dicha contradicción entre los requisitos necesarios de los servicios digitales contenidos en el primer párrafo de la norma con el listado contenido en el segundo párrafo de esta, es posible identificar dos interpretaciones sobre la lectura que debe darse al listado indicado:

- a. **Primera interpretación:** Basada en una lectura sistemática y finalista de los dos primeros párrafos de la norma, los supuestos del listado solo calificarían como digitales si es que cumplen con los requisitos generales previstos en el primer párrafo de la norma.
- b. **Segunda interpretación:** Basada en una lectura literal del segundo párrafo de la norma, los supuestos del listado calificarán como digitales por el simple hecho de estar comprendidos en dicho listado sin perjuicio de que no cumplan con los requisitos necesarios previstos en el primer párrafo de la norma.

Habiendo referido ambas interpretaciones pasamos a analizar los fundamentos que la sustentan en el punto siguiente.

III. Análisis técnico de las interpretaciones del Artículo 4-A del Reglamento

- i. **Primera interpretación: Los supuestos del listado solo calificarían como digitales si es que cumplen con los requisitos generales previstos en el primer párrafo de la norma**

Esta interpretación se sostiene en una lectura sistemática e integral de los dos primeros párrafos del inciso b) del artículo 4-A del Reglamento de la Ley del IR¹⁰. Mientras el primero establece los requisitos esenciales para que un servicio califique como digital, el segundo cumple un rol ejemplificativo, sin capacidad definitoria autónoma.

¹⁰ Artículo 4-A.- “(...) b) **Se entiende por** servicio digital **a** todo servicio que se pone a disposición del usuario a través del Internet o de cualquier adaptación o aplicación de los protocolos, plataformas o de la tecnología utilizada por Internet o cualquier otra red a través de la que se presten servicios equivalentes mediante accesos en línea y que se caracteriza por ser esencialmente automático y no ser viable en ausencia de la tecnología de la información. Para efecto del Reglamento, las referencias a página de Internet, proveedor de Internet, operador de Internet o Internet comprenden tanto a Internet como a cualquier otra red, pública o privada.” (Énfasis agregado).

Por tanto, los servicios enumerados solo calificarán como digitales si cumplen con las condiciones del primer párrafo, entre ellos, **ser** esencialmente automático y contar con una mínima intervención **humana**. Esta interpretación ha sido compartida tanto por el Tribunal Fiscal¹¹ como por el poder Judicial¹².

¹¹ A tal efecto, véase las siguientes Resoluciones del Tribunal Fiscal:

- **05459-8-2018:** El Tribunal Fiscal señaló que, aun si se tratara de un servicio de consultoría, para calificar como servicio digital debe cumplirse con lo previsto en el numeral 7 del inciso b) del artículo 4-A del Reglamento de la LIR. En este caso, no se configuró un servicio digital porque: (i) no se prestó mediante accesos en línea; (ii) no benefició al usuario de forma inmediata; (iii) se evidenció el uso correos y llamadas telefónicas solo como medios de comunicación; y, (iv) el servicio era viable incluso sin tecnologías de la información.
- **09787-4-2019:** Para que un servicio califique como digital bajo el numeral 7 del inciso b) del artículo 4-A del Reglamento de la Ley del IR, debe cumplir con los elementos previstos en la definición general de servicio digital contenida en dicho inciso. En este sentido, el Tribunal Fiscal ha señalado que, en el caso analizado, los servicios prestados no califican como digitales, al no haberse puesto a disposición del usuario mediante accesos en línea ni haberse ejecutado de forma inmediata, limitándose los correos electrónicos enviados a ser un medio de comunicación. Asimismo, precisó que los infirmes emitidos por la Administración Tributaria, como el 018-2008-SUNAT/2B0000, no resultan vinculantes para el Tribunal, conforme al artículo 94 del Código Tributario.
- **07221-1-2020:** “(...), a fin de que se configure el servicio digital previsto en el numeral 7 del inciso b) del artículo 4-A del Reglamento de la Ley del IR, se debía cumplir con los elementos establecidos en la definición prevista en el citado inciso b) del Artículo 4-A del Reglamento de la Ley del IR. (...) en cuanto a lo manifestado por la Administración sobre (...) que la rapidez con la que se ejecuta el servicio en relación con el requerimiento del usuario no es determinante para que se considere la existencia de un acceso en línea, **sustentándose en el Informe N° 018-2008-SUNAT/2B0000, es del caso anotar que el mismo no resulta vinculante para este Tribunal, sino únicamente para la Administración, según el Art. 94 del C.T.**”

¹² A tal efecto, véase las siguientes sentencias de Casación:

- **16003-2003-LIMA:** “(...) **no es admisible la interpretación literal y aislada que postula la SUNAT**, ya que el ordenamiento tributario debe ser comprendido como un sistema normativo, cuya interpretación exige coherencia con los supuestos legales que lo estructuran. Así, los servicios mencionados en el numeral 7 del literal b) del Artículo 4-A del Reglamento debe ser leídos de forma sistemáticas con los requisitos generales del mismo Artículo, evitando interpretaciones arbitrarias o carentes de sustento jurídico.”

ii. Segunda interpretación: los supuestos del listado calificarán como digitales por el simple hecho de estar comprendidos en dicho listado sin perjuicio de que no cumplan con los requisitos necesarios previstos en el primer párrafo de la norma

Esta interpretación se basa en una lectura literal del segundo párrafo del artículo 4-A del Reglamento de la Ley del IR, asumiendo que los servicios incluidos en el listado califican como digitales por el solo hecho de estar expresamente mencionados, incluso si no cumplen con los requisitos establecidos en el primer párrafo.

Esta postura, fue sostenida por la SUNAT en los Informes 018-2008-SUNAT/2B0000¹³ y 039-2024-SUNAT/7T0000, mediante los cuales se sostuvo una interpretación aislada de los supuestos contenidos en el listado del Reglamento por sobre los requisitos generales para calificar un servicio como digital.

A mayor abundamiento, en el Informe 039-2024-SUNAT/7T0000 la Administración Tributaria sostuvo que un servicio califica como digital por el solo hecho de estar incluido en el listado del Reglamento, aun cuando no cumpla con los requisitos del primer párrafo. En esa línea, consideró como digitales servicios como el soporte técnico brindado por técnicos a través de plataformas o correo electrónico, limitando su gravamen únicamente a su uso económico en el país.

-
- **2705-2024-LIMA:** Estos servicios no califican como digitales sujetas a retención del 30%, por las siguientes razones: (i) aunque el Reglamento incluye servicios como soporte técnico en red y consultoría vía correo electrónico o videoconferencia, estos solo se consideran digitales si cumplen con los requisitos generales de la norma; (ii) uno de dichos requisitos es que el servicio sea esencialmente automático, es decir, dependiente de la tecnología y con mínima intervención humana; y, (iii) por tanto, el uso de correo electrónico u otros medios remotos no basta por sí solo para calificar el servicio como digital, si no cumple con los elementos esenciales previstos en la normativa.

¹³ **Informe 018-2008-SUNAT/2B0000:** “El Reglamento, al indicar que el servicio se pone a disposición mediante accesos en línea, se refiere a que el servicio se presta al usuario mediante conexión a la red, tal como se desprende de las definiciones citadas anteriormente, pero **no implica necesariamente que el servicio sea prestado mediante una respuesta inmediata a un requerimiento.** Ello implica que es determinante para calificar un servicio como digital el medio

Los principales fundamentos de la Administración Tributaria para arribar a dicha conclusión podrían ser resumidos de la siguiente forma:

- El Reglamento de la Ley del IR ha contemplado expresamente los supuestos consultados como servicios digitales, por lo que califican como tales en base a una interpretación literal.
- Estos servicios han sido calificados como digitales en base a los documentos emitidos por la OCDE.
- Por tanto, los supuestos de la lista del Reglamento de la Ley del IR deben ser leídos de forma aislada o separada porque han sido regulados de forma expresa como servicios digitales.
- Los requisitos esenciales solo aplican a supuestos distintos de los que aparecen en la lista del Reglamento de la Ley del IR.

Al respecto, el 08 de mayo del 2025 se publicó el Informe 046-2025-SUNAT/7T0000, mediante el cual la Administración tributaria dejó sin efecto la postura antes descrita y con ella la interpretación literal del Reglamento de la Ley del IR. Aunque cuando ello es así, consideramos importante brindar nuestro punto de vista, a efectos de dirimir la controversia en base a una lectura que se sustente en base a una lectura técnica de la norma que regula el tratamiento de los servicios digitales sin perjuicio de la arribada por la Administración Tributaria.

a través del cual se accede a la prestación del servicio (conexión a la red), pero no la forma cómo se procesa la información, esto es, mediante un procesamiento inmediato o 'en batch'. **A manera de ejemplo podemos citar que el numeral 7 del inciso b) del artículo 4º-A del Reglamento**, considera como 'servicios digitales' al acceso electrónico a servicios de consultoría, por el cual se pueden proveer servicios profesionales (consultores, abogados, médicos, etc.) a través del correo electrónico, video conferencia u otro medio remoto de comunicación.

Ahora bien, la prestación de este servicio no se da siempre en línea (de manera inmediata) pues por el contenido de la consulta, el procesamiento de la misma para dar una respuesta puede tardar, con lo que la prestación es mediata.

Sin embargo, el Reglamento ha calificado al acceso electrónico a servicios de consultoría como un servicio digital a pesar de no necesariamente originar una respuesta al usuario de forma inmediata, lo cual evidencia que la rapidez con la que se ejecuta el servicio en relación con el requerimiento del usuario no es determinante para que se considere la existencia de un acceso en línea." (Énfasis agregado).

iii) Nuestra posición

Desde nuestro punto de vista, la interpretación sistemática y finalista, que exige que los servicios incluidos en el listado del Reglamento califiquen como digitales solo si cumplen con los requisitos generales previstos en el primer párrafo del Artículo 4-A, es la que presenta mayor solidez técnica y jurídica. Esta lectura es la compartida por el Tribunal Fiscal y el Poder Judicial, y pareciera guardar coherencia con la reciente rectificación de posición de la SUNAT (Informe Nro. 046-2025-SUNAT/7T0000).

A continuación, presentamos los fundamentos que la sustentan:

A. Con relación a la primera interpretación referida a que los supuestos del listado solo calificarían como digitales si es que cumplen con los requisitos generales previstos en el primer párrafo de la norma, debemos señalar lo siguiente:

- **Coherencia normativa:** Una lectura integral del Artículo 4-A revela que el primer párrafo cumple una función definitoria, estableciendo requisitos esenciales como la automatización del servicio y la dependencia tecnológica. Solo aquellos servicios que superen este umbral pueden ser evaluados a la luz del listado ejemplificativo del segundo párrafo.
- **Soporte en fuentes internacionales:** El documento de la Comisión Europea que sirvió de base para la regulación peruana excluye expresamente como servicios digitales aquellos que requieren intervención humana sustancial, como, por ejemplo, la consultoría profesional prestada por correo electrónico.
- **Conexión con la *ratio legis*:** La regulación de los servicios digitales responde a la necesidad de gravar servicios que, por su naturaleza automatizada, dificultan la aplicación de los criterios tradicionales de conexión territorial. Incluir servicios con intervención humana desnaturaliza este objetivo y puede resolverse aplicando normas ya existentes.
- **Principio de neutralidad tributaria:** Garantizar que la calificación de un servicio como digital responda a su verdadera naturaleza y no únicamente al medio utilizado para su prestación.

En suma, consideramos que, la interpretación sistemática asegura la coherencia interna del ordenamiento, respeta el contexto normativo y doctrinario en el que se dictó la norma, lo que corrobora su validez técnica. Además, es la posición compartida a nivel jurisprudencial.

B. Con relación a la segunda interpretación referida a que los supuestos del listado calificarán como digitales por el simple hecho de estar comprendidos en dicho listado sin perjuicio de que no cumplan con los requisitos necesarios previstos en el primer párrafo de la norma, consideramos que carece de validez técnica en base a lo siguiente:

- Se basa en una lectura aislada de los párrafos del Artículo 4-A del Reglamento, sin reconocer la función definitoria del primer párrafo ni el carácter ejemplificativo del listado.
- Invierte el orden lógico de interpretación normativa, al priorizar el listado de ejemplos sobre la definición general, ello, contradice principios elementales de la hermenéutica jurídica.
- Ignora que las fuentes citadas en la exposición de motivos- especialmente los documentos de la OCDE- describían operaciones generales de comercio electrónico, muchas de las cuales no cumplen con las características esenciales para ser consideradas servicios digitales.
- Desconoce que el documento más idóneo para definir los servicios digitales es el emitido por la Comisión Europea, el cual excluye expresamente a aquellos que implican una intervención humana significativa, como los servicios de consultoría o soporte técnico por correo electrónico.
- Desnaturaliza la *ratio legis* de la norma, al permitir calificar como digitales servicios cuya prestación pueden vincularse claramente a un espacio físico, sin presentar las dificultades de conexión que justifiquen una regulación especial.
- Calificar un servicio como digital únicamente por el medio de prestación - y no por su naturaleza- vulneraría la equidad fiscal y contravendría la finalidad de la norma, toda vez que, se pretendería generar una carga fiscal diferente a determinados contribuyentes en base al medio empleado para realizar sus operaciones y no en base a su capacidad contributiva¹⁴.

¹⁴ En esta línea, podemos indicar el siguiente enunciado de la doctrina:
"Cuando la norma aluda a que el servicio <<se pone a disposición>> del usuario mediante un acceso en línea, se refiere a que es el contenido mismo del servicio el que se traslada, se reparte, se distribuye o se presta al usuario a través de esa vía. Ocurredida alguna de esas acciones, el usuario usa, consume o se beneficia

El análisis de ambas interpretaciones ha permitido evidenciar que solo una lectura sistemática e integral del artículo 4-A del Reglamento de la Ley del IR garantiza coherencia normativa, respeto por la finalidad del legislador y aplicación del principio de neutralidad tributaria. Esta interpretación, que exige el Tribunal Fiscal y el Poder Judicial, y como pareciera desprenderse en el reciente Informe 046-2025-SUNAT/7T0000¹⁵.

IV. Sobre el reciente cambio de criterio emitido por la SUNAT

Como hemos indicado, la Administración Tributaria pareciera haber cambiado su posición mediante la emisión del Informe Nro. 046-2025-SUNAT/7T0000, en el cual, deja de lado la interpretación literal descrita en la segunda posición del punto anterior.

Sin embargo, en este Informe no se ha realizado un análisis detallado de las razones técnicas fundamentadas en una lectura sistemática y finalista como se ha hecho en el presente documento, por lo que, sin perjuicio de su emisión, somos de la opinión de que existen argumentos técnicos que sustentan la primera posición según lo desarrollado.

del servicio. En efecto, <<poner a disposición>> el servicio no significa que la comunicación o la conexión de entrada es electrónica sino que el servicio completo se distribuye por ese medio, lo que ha permitido al usuario consumirlo.

Ello implica que no podría configurar un servicio digital aquél cuya primera conexión se realiza por medios electrónicos mediante acceso, por ejemplo a Internet, pero que origina que el servicio mismo (ej. procesamiento de información) se realice en forma física y se transmita por un medio mecánico o físico como por ejemplo, el teléfono o el fax. En ese caso, el <<servicio>> (el procesamiento de datos) no se <<habría puesto a disposición>> del usuario a través de un acceso electrónico. El Internet habría sido utilizado como un medio de comunicación inicial, pero el servicio mismo habría sido realizado en forma física o manual. Nótese que, además, un caso como el descrito, no podría configurar como servicio digital, toda vez que dicha operación no constituiría una de comercio electrónico directo sino indirecto.”

Muñoz Salgado, Silvia María. “Los servicios digitales como supuesto de renta de fuente peruana”. En: X Jornadas Nacionales de Derecho Tributario. Instituto Peruano de Derecho Tributario. Lima, 2008, p. 181.

¹⁵ Informe de SUNAT que reconoce que servicios con intervención humana significativa- como el soporte técnico y la consultoría profesional- no califican como digitales si no cumplen con los criterios de automatización y dependencia tecnológica.

Ahora, si bien la SUNAT ha adoptado recientemente una interpretación coherente con el enfoque sistemático del artículo 4-A del Reglamento de la Ley del IR –el cual es vinculante es para los funcionarios de la SUNAT, en virtud del artículo 94 del Código Tributario¹⁶–, es importante que los servicios prestados por sujetos no domiciliados que no reúnen las condiciones necesarias para ser calificados como digitales, se encuentren debidamente sustentados con documentación que acredite su naturaleza.

En efecto, si bien la Administración Tributaria pareciera haber dejado sin efecto su lectura literal del Reglamento de la Ley del IR, es importante que, en una eventual fiscalización iniciada por dicha entidad, el contribuyente acredite el no cumplimiento de alguno de estos requisitos para sustentar la no configuración de un supuesto de renta de fuente peruana sujeta a retención del IR.

Así, si se tiene un servicio de consultoría brindado por un profesional ubicado en el extranjero, se debe de contar con documentación que acredite que el servicio no resulta esencialmente automático al tener una preponderante intervención humana. En ese sentido, podría recopilarse una redacción clara del contrato que establezca su forma de prestación y la intervención de un profesional competente, actas de reuniones llevadas a cabo de forma virtual en tiempo real, correos electrónicos que evidencien la materialización de la consultoría, presentaciones elaboradas por el consultor que evidencia una intervención humana, entre otros, de carácter similar.

En suma, si bien el nuevo criterio constituye un avance técnico en el tratamiento de los servicios prestados por proveedores no domiciliados, resulta fundamental que las compañías cuenten con un sustento documentario sólido que les permita acreditar la verdadera naturaleza de sus operaciones. Ello no solo las posicionará de mejor manera frente a un eventual procedimiento de fiscalización tributaria, sino que también contribuirá a mitigar los riesgos de controversias en instancias superiores.

¹⁶ Artículo 94 del Texto Único Ordenado del Código Tributario (Decreto Supremo 133-2013-EF), que establece que los informes emitidos por la SUNAT son obligatorios para los órganos de la propia Administración Tributaria en tanto no sean modificados o dejados sin efecto.

V. Conclusiones

La regulación de los servicios digitales ha presentado durante años una ambigüedad interpretativa en torno al Artículo 4-A del Reglamento de la Ley del IR, particularmente respecto a si el listado reglamentario debe ser leído de forma integrada o aislada.

El análisis técnico desarrollado demuestra que solo una interpretación sistemática –que exige el cumplimiento previo de los requisitos esenciales establecidos en el primer párrafo– garantiza coherencia normativa y respeto por la finalidad de la norma.

Esta interpretación se alinea con los documentos internacionales que sirvieron de base para regulación, en especial el emitido por la Comisión Europea, que excluye servicios con alta intervención humana como la consultoría profesional.

Los pronunciamientos emitidos por el Tribunal Fiscal y el Poder Judicial permiten evidenciar que el listado del Reglamento tiene carácter ejemplificativo y debe interpretarse a la luz de los requisitos generales.

Mediante el Informe Nro. 046-2025-SUNAT/7T0000, la SUNAT ha rectificado oficialmente su criterio asumido en un informe anterior, dejando sin efecto una lectura aislada del listado contenido en el Reglamento de la Ley del IR.

Sin perjuicio de dicho cambio de criterio, es importante analizar el tema en base a una interpretación sustentada en base técnica que sea coherente con la ratio legis, que respete la naturaleza automatizada del servicio, y no en el simple medio de prestación.

En términos prácticos, es importante que las empresas cuenten con documentación de sustento que les permita acreditar la real naturaleza de las operaciones ante un eventual procedimiento de fiscalización tributaria.

¿Árbitros *black box*? Los límites al uso de la inteligencia artificial generativa en arbitrajes bajo el principio de indelegabilidad de la función arbitral

Danae Lucienn Ramos Granados*

Resumen.- La integración de la inteligencia artificial generativa en la práctica del arbitraje internacional ha catalizado un complejo debate sobre su compatibilidad con la integridad del proceso arbitral, específicamente, con la naturaleza *intuitu personae*, en atención a los posibles escenarios de delegación prohibida de las funciones inherentes al árbitro a estas herramientas digitales, trasgrediendo el principio de indelegabilidad de la función arbitral.

Palabras clave: Naturaleza *intuitu personae* – principio de indelegabilidad – funciones arbitrales – inteligencia artificial generativa – designación de árbitros – proceso de toma de decisiones – secretario arbitral.

Abstract.- The integration of generative artificial intelligence in the practice of international arbitration has catalyzed a complex debate on its compatibility with the integrity of the arbitral process, specifically with the *intuitu personae* nature, regarding the possible scenarios of prohibited delegation of the arbitrator's inherent functions to these digital tools, transgressing the principle of non-delegability of the arbitral function.

Keywords.- *Intuitu personae* nature – principle of non-delegability – arbitral functions – generative artificial intelligence – appointment of arbitrators – decision-making process – tribunal secretary.

* Egresada de la Facultad de Derecho de la Pontificia Universidad Católica del Perú (PUCP). Asistente de Investigación en el *Berkeley Center on Comparative Equality & Anti-Discrimination Law* (BCCE) de la University of Berkeley, California. Asistente de cátedra de Derecho Internacional Privado en la PUCP. Miembro del Consejo Editorial de la Revista *Ius Inter Gentes*. Exeditora en jefe de *Themis-Revista de Derecho*.

I. Introducción

El establecimiento de la Inteligencia Artificial (IA) como una herramienta eficiente para la elaboración, revisión y análisis de textos ha generado un incipiente debate acerca de sus potenciales efectos en múltiples disciplinas, tanto beneficiosos como perjudiciales. El derecho no se exime de aquello.

Particularmente, el impacto del uso de Inteligencia Artificial Generativa (IA Generativa) en las labores ejercidas por los tribunales arbitrales ha originado controversia en razón de, por un lado, las potenciales implicancias en atención al debido proceso y, por otro lado, los considerables beneficios en virtud de la celeridad y eficiencia.

Estas herramientas están siendo aplicadas por abogados y árbitros para asistir en labores propias de la profesión. Dentro de ellas se encuentran, por ejemplo, la obtención de borradores o plantillas de documentos legales, la búsqueda de doctrina y jurisprudencia, la revisión gramatical de textos, el resumen de determinados documentos, entre otras. El espectro de acciones que pueden realizarse mediante la IA es interminable.

Esto evidencia que, si bien la IA no es una herramienta insólita, en virtud de que han transcurrido algunos años desde su creación y primer lanzamiento al mercado, sus implicancias se han ido exhibiendo gradualmente. Una de ellas es el uso de la IA Generativa para asistir a los tribunales arbitrales en el desarrollo de un proceso arbitral.

En este marco, dado que los árbitros han comenzado a incorporar las herramientas de IA Generativa en su práctica, ha suscitado preocupación sobre sus potenciales implicancias en la integridad del proceso. Por ejemplo, la vulneración de la confidencialidad, del deber de motivación, del deber de deliberación o, más primigeniamente, del principio de indelegabilidad de las funciones arbitrales.

Si bien a nivel de *soft law* han surgido algunas directrices institucionales y guías de reconocidas instituciones que establecen lineamientos para abordar aquella práctica, hasta este momento no existe aún un criterio instituido a nivel jurisprudencial sobre este particular supuesto, ni legislación que haya decidido regular el uso de la IA Generativa en procesos arbitrales.

A partir de ello, resulta legítimo plantear las siguientes interrogantes: ¿cuáles son los estándares y restricciones que deberían orientar la actuación de los árbitros cuando se asisten de una IA? ¿Puede el uso de IA por parte de un árbitro constituir una forma de delegación prohibida de la función arbitral?

II. El carácter *intuitu personae* de la función arbitral y el principio de indelegabilidad

i. Conceptualización

Como se ha observado, la evolución tecnológica puede plantear desafíos para la integridad del proceso arbitral, especialmente en lo que respecta al principio de indelegabilidad, que constituye una manifestación del carácter *intuitu personae* de la función del árbitro.

¿Qué implica la naturaleza *intuitu personae*? Esencialmente, que el árbitro debe desempeñar personalmente las funciones para las que fue designado. Constituye una garantía fundamental del arbitraje, conllevando la prohibición de delegar o externalizar a otros sujetos los aspectos inherentes a sus labores (indelegabilidad), tales como realizar la evaluación de pruebas documentales, atender las audiencias o, más fundamentalmente, adoptar una decisión sobre la controversia.

En 1969, el profesor Frederic Eisemann había considerado lo siguiente sobre la misión de los árbitros: “ningún árbitro puede delegar su tarea en una tercera persona, ya que la misión de árbitro le ha sido conferida *intuitu personae*”¹. Luego, en 1985, el profesor René David describió aquella característica del siguiente modo:

El árbitro fue elegido *intuitu personae*, porque las partes confiaban en él o estaban dispuestas a someterse a su autoridad; (...) de quien se esperaba que fuera capaz de idear una solución satisfactoria para una controversia².

¹ “No arbitrator can assign his task to a third person, the mission of arbitrator having been conferred upon him *intuitu personae*” (texto original). EISEMANN, F. (1969). *Déontologie de l'Arbitrage Commercial International*. *Revue de l'Arbitrage*, 4, 217-229, p. 229.

² “The arbitrator was chosen *intuitu personae*, because the parties trusted him or were prepared to submit to his authority; (...) of whom it was expected that he would be able to devise a satisfactory solution for a dispute” (texto original). DAVID, R. (1985). *Arbitration in International Trade*. Kluwer Law International, p. 29.

En este sentido, es evidente que la misión otorgada por las partes al árbitro es personalísima. Y ello se explica dado que la propia decisión de las partes que le confiere aquel mandato también es personalísima. Constituye, por ende, un axioma³ y es de tal trascendencia que, no solamente se puede considerar como un principio del arbitraje, sino también como una obligación que no es objeto de discusión en la doctrina⁴.

Ahora bien, en tanto el carácter *intuitu personae* implica que, de manera única y excluyente, es el árbitro el que debe ejercer su función, el correlato negativo es que aquella no puede ser delegada a algún tercero, es decir, el principio de indelegabilidad. El origen de aquella obligación radica en la confianza que las partes han depositado en los árbitros y en sus capacidades. En atención a ello, se les adjudican las competencias para resolver el conflicto. Aquella relación puede explicarse del siguiente modo:

La resolución de una controversia por parte de un árbitro es una obligación personalísima al consistir en una actividad intelectual en función de sus conocimientos, especialidad, experiencia, disponibilidad, etc. Cualidades todas ellas infungibles que contribuyen al carácter indelegable de las obligaciones *intuitu personae* del árbitro⁵.

Entonces, la razón detrás de la importancia del principio de indelegabilidad está en que las partes, en virtud de su autonomía, han designado libremente a determinados individuos (árbitros) para que, en

³ “It is axiomatic to say of an arbitrator’s mission that it is ‘*intuitu personae*’. A party’s choice of arbitrator is, of essence, personal. And so is the chosen arbitrator’s mandate. In accepting appointment, an arbitrator necessarily accepts a duty not to delegate that mandate” (texto original). PARTASIDES, C. (2002). The Fourth Arbitrator? The role of secretaries to tribunals in international arbitration. *Arbitration International*, 18(2), 147-163, p. 147.

⁴ “In a general sense, there is no debate as to whether arbitrators have a duty with regard to personal performance. An arbitrator’s mandate arises from the disputing parties’ exercise of their own autonomy, and is therefore viewed as an *intuitu personae* question” (texto original). FACH GÓMEZ, K. (2019). *Key Duties of International Investment Arbitrators: A Transnational Study of Legal and Ethical Dilemmas*. Springer International Publishing, p. 123.

⁵ MUNNÉ, F. (2002). *La administración del arbitraje: Instituciones arbitrales y procedimiento arbitral*. Aranzadi, p. 22.

función de su propio criterio, conocimiento y experiencia, resuelvan un conflicto, ejerciendo su propia actividad intelectual y decisoria. En este escenario, surge una pregunta esencial: ¿puede el uso de IA por parte de un árbitro constituir una forma de delegación prohibida y, por ende, una violación al principio de indelegabilidad?

De hecho, la selección de árbitros es una de las características esenciales del arbitraje. A diferencia de la justicia estatal, aquí prima la libertad de las partes en designar quiénes los van a juzgar, dado que son ellas las que están en mejor posición de seleccionar quiénes tienen mayor competencia para aquel encargo: conocen directamente y a profundidad su relación jurídica, los disensos derivados de su disputa y los requerimientos de su caso particular. En cambio, el juez es designado de forma aleatoria y tiene un mandato permanente.

De este modo, los profesores Gaillard y Savage consideran que “Los árbitros son jueces privados y, como tales, pueden ser elegidos por ciertas cualidades que poseen o por su experiencia en un campo concreto”⁶. Y lo mismo ha reconocido el profesor Gary Born:

Una de las características y atractivos que definen el proceso arbitral es la capacidad de las partes para seleccionar un tribunal que resolverá su controversia de manera competente y experta, en lugar de depender de la selección aleatoria de un juez de un tribunal nacional. Para lograr este proceso, es esencial determinar de primera mano cuál es la experiencia, el compromiso, la capacidad y la disponibilidad reales de un posible árbitro⁷.

⁶ “Arbitrators are private judges, and as such they may be chosen because of certain qualities they possess, or for their experience in a particular field” (texto original). GAILLARD, E. & SAVAGE, J. (1999). Fouchard, Gaillard, Goldman on International Commercial Arbitration. Kluwer Law International, p. 576.

⁷ “One of the defining characteristics and attractions of the arbitral process is the party’s ability to select a tribunal that will decide their dispute in a competent, expert manner, rather than relying on random selection of a national court judge. Essential to achieving this process is determining, first-hand, what a prospective arbitrator’s actual experience, commitment, capability and availability are” (texto original). BORN, G. (2021). International Commercial Arbitration (3rd Ed.). Kluwer Law International, p. 2780.

En este sentido, la designación de árbitros es uno de los principales motivos para acudir al arbitraje⁸ y un pilar esencial del sistema. Al ser los árbitros designados según sus cualidades personales, deben ser ellos –de manera exclusiva y excluyente– los que desempeñen las funciones que les han sido asignadas (*intuitu personae*).

ii. Estándares de protección

Una de las primeras instituciones en regular esta obligación fue la American Arbitration Association (AAA) en el 2004, al emitir su “*Code of Ethics for Arbitrators in Commercial Disputes*”, donde se establece que “Un árbitro no debe delegar la facultad de decidir en ninguna otra persona”⁹. La prohibición es directa: el deber de decisión recae únicamente en el árbitro y no puede ser delegado.

En el 2014, la International Council for Commercial Arbitration (ICCA) emitió la “*Young ICCA Guide On Arbitral Secretaries*” que busca establecer buenas prácticas para la designación y el uso de secretarios arbitrales. Entre ellas, se encuentran las siguientes:

Artículo 1. Principios generales sobre el nombramiento y uso de secretarios arbitrales

(1) Deberá nombrarse un secretario arbitral para apoyar al tribunal arbitral cuando éste considere que dicho nombramiento le ayudará a resolver la controversia de manera efectiva y eficiente.

(2) Un secretario arbitral sólo debe ser nombrado con el conocimiento y consentimiento de las partes.

(3) El tribunal arbitral deberá notificar a las partes su intención de nombrar un secretario arbitral a la mayor brevedad posible.

⁸ Esto ha sido confirmado en una encuesta de la Queen Mary University of London, donde el 39% confirmó que “the ability of parties to select arbitrators” es la característica más valiosa del arbitraje. La encuesta del 2015 tuvo resultados similares. Véase: <https://www.qmul.ac.uk/arbitration/research/2018/>.

⁹ “An arbitrator should not delegate the duty to decide to any other person”. American Arbitration Association (AAA) (2004). *Code of Ethics for Arbitrators in Commercial Disputes*. P. 6. https://www.adr.org/sites/default/files/document_repository/Commercial_Code_of_Ethics_for_Arbitrators_2010_10_14.pdf.

(4) Será responsabilidad de cada árbitro no delegar ninguna parte de su mandato personal en ninguna otra persona, incluido un secretario arbitral.

(5) Será responsabilidad del tribunal arbitral seleccionar adecuadamente y supervisar al secretario arbitral (...) ¹⁰.

Se enfatiza la obligación de contar con el consentimiento de las partes, y a que exista una verdadera necesidad de apoyo, aspectos particulares en comparación con otras directrices. Asimismo, se establece que no podrá delegarse “ninguna parte de su mandato personal”, es decir, las funciones inherentes de su rol como árbitro.

Posteriormente, la Cámara de Comercio Internacional (CCI) emitió la “Nota de la CCI a las partes y a los tribunales arbitrales sobre la conducción del arbitraje” (2021), en donde establece obligaciones y reglas vinculadas con la designación de los secretarios:

222. Los secretarios administrativos actúan de conformidad con las instrucciones del tribunal arbitral y bajo su estricta y continua supervisión. El tribunal arbitral es responsable en todo momento de la conducta del secretario (...).

223. Bajo ninguna circunstancia el tribunal arbitral puede delegar sus funciones de toma de decisiones en el secretario administrativo ni contar con un secretario administrativo para la realización en su nombre de cualquiera de las obligaciones esenciales de un árbitro. Igualmente, las funciones asignadas a un secretario administrativo, tales como la preparación de notas por escrito o memorandos, no eximirán al tribunal arbitral de su obligación de revisar personalmente el expediente y/o redactar él mismo cualquier decisión del tribunal arbitral ¹¹.

Como se observa, la responsabilidad final siempre recaerá en el árbitro, quien deberá cumplir con tres obligaciones: (1) no delegar sus funciones de toma de decisiones al secretario, (2) no encomendar sus labores esenciales al secretario y (3) supervisar la actuación del secretario y

¹⁰ Véase: <https://www.arbitration-icca.org/icca-reports-no-1-young-icca-guide-arbitral-secretaries>

¹¹ Véase: <https://www.iccspain.org/wp-content/uploads/2024/02/icc-note-to-parties-and-arbitral-tribunals-on-the-conduct-of-arbitration-spanish-2021.pdf>

hacerse responsable de su conducta. Se afirma que el secretario puede redactar “notas escritas o memorandos”, sin que eso exima al árbitro del deber de revisión personal y final o, en todo caso, de redactar por sí mismo la decisión.

Más recientemente, la United Nations Commission on International Trade Law (UNCITRAL) publicó su “Código de Conducta de la CNUDMI para Árbitros en la Solución de Controversias Internacionales Relativas a Inversiones” (2024), donde establece:

Artículo 6. Integridad y competencia

(...) Prohibición de delegar funciones decisorias

La adopción de decisiones es la principal función de un árbitro y, por lo tanto, no puede delegarse. Sin embargo, el apartado c) no impide que un árbitro solicite a su asistente que prepare, bajo su dirección, partes de borradores preliminares de la decisión o laudo, siempre que esos borradores sean cuidadosamente examinados por él, de modo que el texto final refleje el razonamiento y la decisión del árbitro y no los de su asistente (inciso 47).

Artículo 10. Asistente

(...) Contratación de un asistente

70. En general, entre las tareas que lleva a cabo un asistente figuran la realización de investigaciones jurídicas, el examen de los alegatos y la prueba, la logística del caso, la asistencia a las deliberaciones y otras tareas similares. Cuando se encomiende a un asistente que prepare partes de borradores preliminares de la decisión o laudo, deberá realizar siempre esas tareas según las instrucciones del árbitro y bajo su dirección, y no debería ejercer ninguna función decisoria¹².

Así, la existencia del principio de indelegabilidad no implica que no pueda haber participación de un tercero que redacte borradores de laudos, siempre que sea bajo su dirección y examinación. Se dilata la esfera de acción, pues en la nota del ICC se aludía solo a “notas escritas o memorandos”. Sin embargo, el límite es que estos borradores de laudos deben ser revisados cuidadosamente por el árbitro y deben terminar manifestando su propio análisis.

¹² Véase: https://uncitral.un.org/sites/uncitral.un.org/files/mediadocuments/uncitral/es/coc_arbitrators_ebook_s.pdf

En consecuencia, las normas de *soft law* determinan que la obligación de indelegabilidad recae en el proceso de toma de decisiones del árbitro, sin excepciones, y que este asume el deber de revisión y la responsabilidad final frente a cualquier documento elaborado por el secretario.

Como se observa, el efecto típico del principio de indelegabilidad se ha manifestado en poder limitar la incidencia de los secretarios en las funciones esenciales del tribunal. No obstante, cabe analizar la posibilidad de que aquella limitación se pueda extender al uso de *softwares* de IA por parte de los árbitros.

III. Asistencia vs. Delegación: ¿Cuándo la delegación se vuelve prohibida?

La IA es usada en los procesos arbitrales a través de una extensa variedad de acciones. Algunas son mecánicas (OCR, traducción, revisión ortográfica y gramatical); algunas vinculadas al conocimiento (búsqueda de jurisprudencia o doctrina); otras se relacionan con el contenido de los documentos (resumen de textos, *document drafting*, revisión o comparación de documentos); y otras se vinculan a la función decisoria (*drafting* de laudos arbitrales, aplicación de las normas a los hechos o razonamiento jurídico).

Tras haber analizado las implicancias de la indelegabilidad, debe hacerse una relevante distinción entre delegación y asistencia. Mientras que esta última supone un apoyo administrativo, técnico o formal subordinado al control del árbitro, aquella implica ceder alguna función arbitral¹³. Y, si esto último aplica sobre una función arbitral inherente, tal como intelectual o decisoria (decision-making process), se volvería una delegación prohibida.

Existen escenarios en donde la delegación es manifiestamente prohibida: la IA emite una decisión vinculante que se publica sin la supervisión del árbitro o el árbitro aprueba conclusiones jurídicas íntegramente generadas por la IA. Estos supuestos implican que el árbitro no ha sido el autor de la decisión. En este sentido, es útil dividir entre la incidencia

¹³ Según la RAE, “delegar” significa: “Dar la jurisdicción que tiene por su dignidad u oficio a otra, para que haga sus veces o para conferirle su representación”. Véase: <https://dle.rae.es/delegar>

de la IA para (i) apoyar en la decisión o (ii) sustituir la decisión, considerando que esta última, en ninguna circunstancia, puede ser permisible.

Ahora bien, dadas las limitaciones para conocer el proceso de toma de decisiones del árbitro, cabe preguntarnos, ¿cuándo el uso de la IA efectivamente implica un reemplazo de la función arbitral decisoria y, por ende, prohibida?

i. Delegación de las funciones arbitrales en terceros: el secretario arbitral

Como se ha observado, la discusión sobre la delegación de tareas de los tribunales arbitrales no ha tenido su origen en el uso de la IA; sino tiempo atrás, al analizar las funciones de secretarios arbitrales o asistentes en el desarrollo de los procesos.

Actualmente, es común en los arbitrajes internacionales la designación de un secretario, por el tribunal o por la institución. Ello se debe a la necesidad de respaldo ante la complejidad y extensión de determinados casos. Tal como mencionan los profesores Gaillard y Savage:

En los grandes arbitrajes internacionales, la carga de trabajo de los árbitros será considerable. La cantidad de pruebas presentadas, el volumen de los escritos intercambiados y el número y la duración de las audiencias de los testigos suelen ser extremadamente importantes. (...) Como resultado, ahora es habitual en las grandes controversias internacionales seguir la práctica suiza de permitir que el tribunal arbitral nombre a un secretario (...) (1999, p. 683)¹⁴.

El surgimiento de la figura de los secretarios se produjo en Suiza, en 1969¹⁵ y se positiviza luego en el Código Civil de Procedimiento de Suiza

¹⁴ “In large international arbitrations, the arbitrators’ workload will be considerable. The amount of evidence submitted, the size of the memorials exchanged and the number and length of witness hearings are often extremely significant. (...) As a result, it is now common in large international disputes to follow the Swiss practice of allowing the arbitral tribunal to appoint a secretary (...)” (texto original). GAILLARD & SAVAGE, op. cit., p. 683.

¹⁵ Se realizó mediante el Concordat sur l’arbitrage du 27 mars 1969, donde se estableció lo siguiente:

“Art. 15 Secrétaire

1. Avec l’accord des parties, le tribunal arbitral peut désigner un secrétaire.

(artículo 365)¹⁶. Posteriormente, diversas leyes de arbitraje reconocieron la posibilidad de contar con un secretario, tal como la Ley de Arbitraje de Brasil en su artículo 13(5)¹⁷, o el Código de Procedimiento Civil de los Países Bajos en su artículo 1073(2)¹⁸. Por su parte, la Ley de Arbitraje peruana, si bien no establece de manera expresa la posibilidad de designación de un secretario, sí incluye su participación en los costos del arbitraje (artículos 70 y 71)¹⁹. En la misma línea va, por ejemplo, el Código de Procedimiento Civil de Grecia, en su artículo 882(3)²⁰.

Las tareas que puede ejercer un secretario arbitral se encuentran condicionadas a lo administrativo o logístico; por ello, los profesores Gaillard y Savage establecen el siguiente límite: “El secretario prestará esencialmente asistencia administrativa y, obviamente, no podrá sustituir al tribunal arbitral en el proceso de toma de decisiones”²¹. Aquel criterio ha sido compartido por los profesores Redfern y Hunter: “Por ejemplo, el secretario puede organizar la comparecencia de los testigos y verificar que la transcripción refleje con exactitud las declaraciones prestadas.

2. Les articles 18 à 20 sont applicables à la récusation du secrétaire”.

https://www.cvci.ch/fileadmin/CVCI/Juridique/Mediation/Concordat_sur_l_arbitrage.pdf

¹⁶ “Art. 365 Secrétaire.

1.Le tribunal arbitral peut désigner un secrétaire.

2.Les art. 363, al. 1, et 367 à 369 sont applicables par analogie”. https://www.fedlex.admin.ch/eli/cc/2010/262/fr#art_365.

¹⁷ Lei de Arbitragem, Lei Nº 9.307, de 23 de setembro de 1996: “§ 5º O árbitro ou o presidente do tribunal designará, se julgar conveniente, um secretário, que poderá ser um dos árbitros”.

¹⁸ “Artículo 1033. Un árbitro podrá ser recusado si existen dudas justificadas sobre su imparcialidad o independencia. (...) Artículo 1035a. Si el tribunal arbitral está asistido por un secretario, se aplicarán mutatis mutandis los artículos 1033 a 1035” (traducción libre).

¹⁹ Decreto Legislativo 1071, Decreto Legislativo que norma el Arbitraje. (2008).

²⁰ “El laudo arbitral será la determinación final de la remuneración y los gastos del arbitraje, que incluirán la remuneración del secretario” (traducción libre). Decreto Presidencial 503/1985. <https://www.lawspot.gr/nomikes-plirofories/nomothesia/kpold/arthro-882-kodikas-politikis-dikonomias>.

²¹ “The secretary will essentially provide administrative assistance, and obviously cannot replace the arbitral tribunal in the decision-making process” (texto original). Gaillard y Savage, op. cit., p. 683.

Sin embargo, el secretario arbitral no debe participar activamente en las deliberaciones privadas del tribunal arbitral (...)”²².

Un elemento de importancia es contar con el permiso de las partes. Aquello puede implicar una disposición en el convenio arbitral²³; la consulta del tribunal a las partes o, lo que podría ser más usual, que los lineamientos de la institución arbitral correspondiente prevean su participación o funciones. Como veremos más adelante, este consentimiento de las partes y el deber de información del árbitro cobrará especial importancia frente al uso de IA, en tanto el riesgo de su incidencia en el proceso arbitral es mayor.

En el ámbito peruano, por ejemplo, el Reglamento del Centro de Arbitraje de la Cámara de Comercio de Lima (CCL) establece que: “Los secretarios arbitrales tienen la función de asistir a los Tribunales Arbitrales en el desarrollo del arbitraje y, en general, de contribuir con el cumplimiento de las funciones de la Secretaría General, bajo la supervisión del Consejo (...)” (artículo 14).

La London Court of International Arbitration (LCIA) también ha establecido en su reglamento diversas provisiones sobre el *tribunal secretary*:

- El artículo 14.8 autoriza recibir asistencia de un secretario, pero con sujeción al reglamento y a la ley aplicable. No obstante, prohíbe cualquier delegación de la función decisoria del tribunal en el secretario. Cualquier tarea asignada debe realizarse bajo la supervisión directa del tribunal, que seguirá siendo responsable de garantizar que cumplen los estándares exigidos por las reglas.
- El artículo 14.9 establece que el candidato debe declarar las circunstancias que generen dudas justificadas sobre su imparcialidad o independencia.

²² “For example, the secretary may organise the attendance of witnesses and verify that the transcript accurately records the evidence given. However, the arbitral secretary should not take an active part in the private deliberations of the arbitral tribunal (...)” (texto original). Redfern y Hunter, op. cit., p. 301.

²³ Al respecto: “It is important to obtain the agreement of the parties before any appointment is made, with a clear explanation to the parties of the nature of the secretary’s role and the benefits that such an appointment will give to the process, in terms of efficiency and cost savings” (REDFERN & HUNTER, 2015, p. 30).

- El artículo 14.10 establece que el tribunal sólo podrá recibir asistencia cuando las partes hayan dado su aprobación expresa. Se considera válida cuando (i) acuerdan las tareas que realizará el secretario; (ii) acuerdan la tarifa y las condiciones de reembolso; (iii) la declaración se comparte con las partes; y (iv) las partes acuerdan la persona específica propuesta para actuar como secretario²⁴.

La LCIA plantea un estándar más estricto y detallado sobre el papel de los secretarios en comparación con otras normas. Exige la aprobación expresa de las partes, a diferencia de la CCL, y no solo para el nombramiento, sino también para el alcance de sus tareas. Además, prohíbe a los secretarios desempeñar funciones decisorias e impone un deber permanente de supervisión al árbitro. Este modelo refleja un esfuerzo sólido de la LCIA por preservar y fortalecer el principio de indelegabilidad.

En suma, el rol de los secretarios arbitrales se encuentra limitado y supervisado, debido a los diversos riesgos que pueden surgir frente a la desnaturalización de sus labores.

En este punto, es menester observar cuáles son específicamente las labores administrativas realizables por terceros. De acuerdo con la mencionada Nota de la ICC, las tareas que puede ejecutar el secretario administrativo son las siguientes (sin ser una lista exhaustiva):

- Transmitir documentos y comunicaciones en nombre del tribunal arbitral.
- Organizar y mantener el expediente del tribunal arbitral y localizar documentos.
- Organizar audiencias y reuniones y colaborar con las partes en este sentido.
- Redactar correspondencia a las partes y enviarla en nombre del tribunal arbitral.
- Preparar, para que sean examinados por el tribunal arbitral, borradores de órdenes procesales, así como secciones sobre cuestiones de hecho de un laudo, tales como el resumen del procedimiento, la cronología de los hechos y el resumen de las posturas de las partes, siempre que dichas órdenes procesales

²⁴ LCIA Arbitration Rules, 2020, article 14A.

y partes del laudo sean revisadas posteriormente por el tribunal arbitral mismo.

- Asistir a audiencias, reuniones y deliberaciones; tomar notas o minutas, o hacer el conteo de tiempo.
- Realizar búsquedas legales o similares.
- Realizar correcciones y verificar citaciones, fechas y referencias cruzadas en órdenes procesales y laudos, así como corregir errores tipográficos, gramaticales o de cálculo (Nota 224).

Esta nota ofrece un aporte significativo por fijar sin ambigüedad los supuestos específicos en los cuales se permite la intervención del asistente, que podría, *mutatis mutandis*, ser aplicado en la determinación de las funciones que puede o no solicitar al árbitro a la IA.

Por otro lado, existen precedentes arbitrales significativos en los que se ha evaluado si la participación del secretario implicó una incidencia en las funciones arbitrales inherentes. Existió un caso primigenio en 1990, resuelto por la *Cour d'Appel de Paris*, donde se desestimó el recurso dado que no se probó como el secretario habría interferido en el procedimiento:

Los tribunales franceses respaldaron claramente esta práctica en una acción para anular un laudo basada en una supuesta violación del debido proceso y de la igualdad entre las partes, supuestamente causada por la presencia del secretario del tribunal arbitral en algunas de las audiencias y su supuesta interferencia en el procedimiento. El tribunal desestimó la acción y sostuvo que el tribunal “tenía derecho a nombrar un secretario” y que no se había demostrado “cómo había interferido en el procedimiento” (pp. 683-684)²⁵.

De este modo, la Corte confirmó que el tribunal tenía discrecionalidad para señalar un secretario y que la validez de la reclamación exige la existencia de una interferencia del secretario que genere perjuicios.

²⁵ “The French courts clearly endorsed this practice in an action to set aside an award based on an alleged breach of due process and of equality between the parties, purportedly caused by the presence of the secretary of the arbitral tribunal at some of the hearings and his alleged interference in the proceedings. The court dismissed the action and held that the tribunal ‘was entitled to appoint a secretary’ and that it had not been established ‘how he had interfered in the proceedings’” (texto original). *Cour d'Appel de Paris, Compagnie Honeywell Bull S.A. v. Compacacion Bull de Venezuela C.A.*, 21 June 1990, citado en PARTASIDES (2002, p. 148).

Con posterioridad, el caso que marcó un hito fue **Yukos v. Federación Rusa**, saga que inició con la demanda planteada en el 2004 frente a la Corte Permanente de Arbitraje (PCA) por Hulley Enterprises Ltd., Yukos Universal Ltd. y Veteran Petroleum Ltd. (Yukos) y culminó en el 2024, con la conformación de la validez del laudo.

Lo relevante fue la solicitud de anulación del laudo emitido por el tribunal de la PCA en el 2014²⁶. Este establecía que Rusia debía pagar \$50 mil millones en compensación a Yukos, por una expropiación indirecta en violación del Tratado sobre la Carta de Energía (1994). En consecuencia, Rusia solicita la anulación del laudo ante la Corte de Distrito de La Haya²⁷.

Entre los argumentos, Rusia alegó que el rol ejercido por el Sr. Valasek, asistente del tribunal, fue desproporcional, concluyendo que se “violó con ello la regla según la cual los árbitros deben ejercitar sus tareas sustantivas personalmente”, por lo cual el tribunal se habría excedido del mandato conferido, causal de anulación establecida en el Artículo 1065(1)(c) del Código de Procedimiento Civil de los Países Bajos.

Asimismo, Rusia alegó que el tribunal estuvo compuesto por cuatro árbitros y no tres, como había sido inicialmente establecido, dado que los laudos fueron emitidos por el asistente del tribunal, el Sr. Valasek. Esto constituiría un motivo de anulación en virtud del Artículo 1065(1)(b): constitución del tribunal en violación de las normas aplicables.

Las pruebas ofrecidas por Rusia fueron los siguientes:

- El Sr. Valasek habría cargado un desproporcionadamente extenso número de horas en la segunda etapa del proceso (2,625), cuando el promedio fueron 1,661 por árbitro. Y que no implicaba una con-

²⁶ Caso PCA N° 2005-04/AA227. El tribunal, constituido bajo normas UNCITRAL, estuvo conformado por Yves Fortier (Presidente), Charles Poncet (nombrado por demandantes) y Stephen Schwebel (nombrado por Rusia).

²⁷ Corte de Distrito de La Haya (Gerechtshof Den Haag). Caso N° 200.197.079/01. 18 de febrero de 2020.

En el 2016, la Corte de Distrito de La Haya anuló el laudo, argumentando que el tribunal arbitral no tenía jurisdicción, porque Rusia no había ratificado el Tratado sobre la Carta de Energía. Yukos apela. En esa instancia de apelación (Corte de Distrito de La Haya) donde se esboza el debate sustantivo sobre el rol del secretario.

tribución sustancial a la administración y organización del tribunal, pues esto recaía en los dos secretarios, que juntos declararon un total de 5,232 horas. Por ende, tuvo una contribución sustancial en el arbitraje (fundamento 6.6.2.a).

- Solicitaron a dos expertos lingüísticos un estudio sobre la redacción de los laudos. Cada uno examinó tres capítulos y, en función de la “presencia de características de autoría derivadas de escritos anteriores de Valasek y de los tres árbitros”, concluyeron que existía el “95% de certeza de que Valasek escribió al menos entre el 60-70% o al menos el 41% de los capítulos IX, X y XII del laudo final” (fundamento 6.6.2.b).

Frente a ello, Yukos respondió lo siguiente:

- Dado que el Sr. Valasek tuvo un rol sustantivo en la elaboración de los laudos, hubo una supervisión por parte del Tribunal, quien mantuvo la responsabilidad final. Por ende, no hubo incidencia del Sr. Valasek en el proceso de toma de decisiones.
- Solicitaron la evaluación de dos expertos, que criticaron los métodos de los peritos de la contraparte. Señalaron que los laudos son el producto conjunto de varios autores y que los métodos no fueron adecuados para indicar con precisión qué sección proviene de qué autor. Por ende, se objeta que el Sr. Valasek haya redactado grandes partes. Además, no coincidieron en qué partes del texto pueden atribuirse a Valasek con un alto grado de certeza (fundamento 6.6.3).

Finalmente, la Corte de Distrito de La Haya determinó que “no se ha establecido que los argumentos de la Federación Rusa sobre el rol sustantivo de Valasek sean correctos” y que eran problemáticos sus estudios lingüísticos porque “(...) el texto de una decisión escrita por múltiples personas no siempre es obra de un solo autor” (fundamento 6.6.5). Además, que de los informes no se concluye que Valasek haya participado en el proceso de toma de decisiones ni asumido tareas exclusivas de los árbitros²⁸.

²⁸ Además: “Y que tampoco se deriva esa conclusión del trabajo de redacción de Valasek, pues puede que los borradores presentados por él no hayan influido en las decisiones de los árbitros, o incluso que la toma de decisiones de los árbitros haya ocurrido antes”. “Es parte de la experiencia de Chaski y Daelemans analizar,

Sobre la redacción de los borradores de laudo por parte del secretario, y la necesidad de la revisión posterior por parte del árbitro, la Corte establece lo siguiente:

Los textos redactados por un asistente o secretario (o los textos proporcionados para fines del laudo arbitral) pueden estar sesgados o incompletos, incluso si los árbitros han dado instrucciones detalladas sobre su contenido. Sin embargo, corresponde a los árbitros verificar la corrección y exhaustividad de estos textos.

Además, la presentación de estos textos no implica que el asistente haya tomado decisiones independientes que formen parte de la función esencial de los árbitros. Contrario a lo que sostiene la Federación Rusa, el uso por parte del tribunal de borradores redactados por Valasek no equivale a una “abolición total del principio de *intuitu personae*” ni a una violación de la prohibición de delegación. Lo que importa es que los árbitros asumieron la responsabilidad final por los borradores, ya sea que los aceptaran total o parcialmente, con o sin enmiendas (fundamento 6.6.10).

Por último, en lo referido a la violación del mandato, la Corte establece lo siguiente:

La Corte asume que Valasek redactó partes de los laudos que fueron incorporadas por los árbitros, lo cual innegablemente implica trabajo sustantivo. Pero esto no significa, por sí solo, que al delegar esas actividades, los árbitros hayan violado su mandato de forma tan grave que deba anularse el laudo. Las reglas de arbitraje aplicables (Reglas de la CNUDMI) no contienen ninguna provisión en el asunto. Contrario a la opinión de la Federación Rusa, tampoco existe una regla no escrita que impida a un secretario o asistente redactar partes del laudo (...).

En tanto no se ha realizado ningún acuerdo entre las partes en este respecto y las decisiones (sustantivas) son tomadas por los árbitros mismos sin influencia de terceros, debe dejarse a discreción del Tribunal hasta qué punto desea usar un asistente o secretario en la redacción del laudo arbitral (...) (fundamento 6.6.14.1).

utilizando un método científico, qué autor (con mayor probabilidad) escribió cierto texto, pero no para determinar si ese autor lo escribió por su propia cuenta o bajo las instrucciones y responsabilidad de otra persona” (fundamento 6.6.6).

Y sobre la alegación de que las partes no fueron informadas plenamente del rol de Valasek, la Corte considera que tampoco procede anular el laudo por ello, dado que no constituye una violación suficientemente grave del mandato.

En consecuencia, el Tribunal estableció que las funciones ejercidas por el asistente no constituyen ninguna violación del mandato otorgado, ni de la composición del tribunal²⁹. Este caso estableció un precedente fundamental: no habrá violación de la obligación *intuitu personae* si el tribunal mantiene el *decision-making process* y la responsabilidad final del laudo.

Además del conocido caso Yukos, en el 2023, la *Cour de Cassation* de Bélgica resolvió un caso con alegaciones similares³⁰. Se solicitó la anulación de un laudo en un arbitraje CCI, encontrándose, entre los fundamentos, la supuesta delegación indebida de funciones a la secretaria arbitral (redacción del laudo). El tribunal la había designado con observancia al procedimiento establecido en las normas CCI y al consentimiento de las partes³¹.

La Corte confirmó la posibilidad de que los secretarios colaboren con la redacción de notas y memorandas que luego pueden servir de base o formar parte del contenido del laudo. No obstante, siempre debe haber una deliberación personal del tribunal:

La prohibición para el tribunal arbitral de delegar sus funciones jurisdiccionales no impide que el secretario administrativo prepare notas y memorandos que, o bien formarán parte del laudo después de que el tribunal arbitral los haya, sobre la base de su examen personal del expediente, revisado, corregido y validado, o bien servirán de base para

²⁹ ¿Cómo se resolvió el caso? En el 2020, la Corte de Distrito de La Haya revocó la decisión de anulación y restableció el laudo. En el 2021, la Corte Suprema de los Países Bajos devolvió el caso a una corte inferior para revisión, sin anular definitivamente el laudo. Finalmente, en el 2024, la Corte de Apelaciones de Ámsterdam reafirmó la validez. <https://investmentpolicy.unctad.org/investment-dispute-settlement/cases/213/yukos-universal-v-russia>

³⁰ Cour de cassation de Belgique. (2023) Arrêt N° C.21.0548.F. https://juportal.be/JUPORTAwork/ECLI:BE:CASS:2023:ARR.20230424.3F.1_FR.pdf.

³¹ Véase: <https://arbitrationblog.kluwerarbitration.com/2021/08/22/delegation-of-tasks-to-arbitral-secretaries-striking-the-right-balance/>

la elaboración por parte de ese tribunal, tras ese mismo examen personal, del laudo, no otorga a las disposiciones antes mencionadas de la nota litigiosa una interpretación inconciliable con sus términos, y por tanto, no viola la fe debida al acto que las contiene (traducción libre) (2023, p. 5).

Se sigue, por ende, el criterio establecido en Yukos: se debe demostrar que los árbitros cedieron la autoridad inherente de tomar decisiones para la controversia (*decision-making process*), no simplemente que hubo la asistencia de un determinado secretario arbitral.

También se examinó el uso de la expresión “y/o” en el artículo 187 de la referida Nota CCI, señalando que, aunque formalmente se establece que el tribunal no puede delegar su obligación de revisar el expediente ni redactar las decisiones, el empleo de “y/o” permite interpretar que el secretario puede elaborar total o parcialmente un proyecto de laudo, siempre que luego el árbitro realice una revisión. Esta ambigüedad en la redacción, aunada al hecho de que la propia CCI organiza capacitaciones para sus secretarios acerca de la redacción de laudos³², consolida la posibilidad de que participen en la redacción del laudo.

Aplicando la lógica establecida en ambos casos al uso de IA, podríamos concluir en que no habría inconveniente en que la redacción de secciones del laudo sea elaborada por IA, siempre que el árbitro mantenga el *decision-making process* y la responsabilidad final, lo que implicaría la revisión, corrección, y consecuente rechazo o aceptación de aquellos textos.

ii. Delegación de las funciones arbitrales en la IA

Antes de establecer un análisis comparativo entre las funciones de la IA y de un secretario arbitral, es menester evidenciar las distancias intrínsecas que existen entre ambos. Normalmente, el secretario arbitral es un abogado *junior*, que tiene cierta experiencia en el área y ha colaborado

³² Por ejemplo, en el 10th ICC Asia Pacific Conference on International Arbitration hubo una capacitación para secretarios (ICC Institute of World Business Law Training for Tribunal Secretaries), en cuyo programa estaba el módulo de “Solicitudes de producción de documentos: proporcionar copias de los documentos pertinentes al presidente del tribunal, asistir y seguir las deliberaciones al respecto y preparar un proyecto de decisión en el Anexo Redfern bajo la dirección, el control y la supervisión del tribunal”. <https://events2go.iccwbo.org/event/10th-apac-conference-on-international-arbitration>.

en otros casos arbitrales³³. La IA, si bien puede acceder a un sinfín de información (es su rasgo esencial) sobre conocimiento jurídico y de la práctica arbitral, aquello no lo capacita del mismo modo en que lo está un abogado, cuya formación implica la adquisición de competencias sustantivas y deliberativas que un *software* no posee. Ahora bien, es innegable que, en el ámbito de sus facultades, ambos podrán cometer errores.

No obstante, nada impide hacer una similitud válida entre los secretarios arbitrales y la IA, siendo que ambos pueden actuar como **‘terceros’ que asisten o en los que se delegan ciertas funciones** no esenciales en el marco de un proceso arbitral. Por ende, nada obsta a que los estándares establecidos para examinar la legitimidad de la incidencia de los secretarios arbitrales en el transcurso del proceso sean también aplicados, *mutatis mutandis*, a la IA.

Este año, se ha conocido el problema en una demanda interpuesta el 8 de abril de 2025 frente a la U.S. District Court for the Southern District of California (*LaPaglia v. Valve Corporation*)³⁴. En este escrito, el Sr. Lapaglia solicita la anulación de un laudo emitido en favor de Valve Corporation, una empresa de videojuegos. Entre los fundamentos, se encuentra que “el árbitro Saydah externalizó su función de adjudicación a la Inteligencia Artificial (IA)”, lo que implicaría haberse extralimitado de sus facultades, una de las causales de anulación de laudo de acuerdo con el artículo 10(a)(4) de la Federal Arbitration Act (FAA). El demandante alega que se usó la IA para redactar el laudo, suplantando la determinación de los hechos y la función de adjudicación del árbitro. Alegó lo siguiente:

- El árbitro habría admitido ante las partes el uso de IA para la redacción de artículos.
- El árbitro habría admitido que tenía la necesidad de emitir un laudo de forma rápida.
- El laudo tendría signos reveladores de generación de IA, tal como describir hechos falsos (no presentados en el juicio ni el expediente).

³³ “The obvious person to appoint as an arbitral secretary or registrar is a young lawyer with some experience of international commercial arbitration and of the administrative problems (...)” (REDFERN & HUNTER, 2015, p. 302).

³⁴ Case 3:25-cv-00833.

- a. El contenido del laudo tendría una “mezcla de hechos” o “alucinaciones”, como afirmar que el videojuego infantil Roblox tiene “elementos de terror” sin ninguna cita que lo sustente.
 - b. El laudo contendría declaraciones que no constan en el expediente, ni en las pruebas, ni puede probarse de otro modo que no sea mediante IA, como la afirmación de que “el año pasado, Sony y Microsoft se asociaron para explorar soluciones de juegos en la nube y streaming utilizando Microsoft Cloud Azure” y que “existe una importante competencia de China con sus propios desarrolladores y plataformas, así como competencia de empresas estadounidenses, en la carrera por conquistar el mercado chino de juegos de PC” (traducción libre).
- El asistente judicial del abogado del demandante consultó a ChatGPT si esa sección del laudo fue escrita por humanos o por IA, a lo que se respondió que “la redacción incómoda, la redundancia, la incoherencia y las generalizaciones excesivas del párrafo sugieren que el pasaje fue generado por una IA” (traducción libre).

En consecuencia, según la demandante, así como se ha determinado la anulación de laudos por delegación en personas distintas al árbitro, también debe aplicar cuando la toma de decisiones se delega en la IA. El caso aún no ha sido resuelto; no obstante, ofrece un importante alcance sobre cómo las partes en el arbitraje consideran el potencial uso de IA durante y después de culminado el arbitraje, y en qué escenarios lo pueden considerar como una violación del principio de indelegabilidad.

IV. Directrices, mecanismos de control y responsabilidad de los árbitros

Si bien este tema es incipiente, diversas instituciones han publicado directrices que permiten establecer cómo debe ser el uso de la IA en los procesos arbitrales. Se coloca un especial énfasis en la independencia e imparcialidad, el deber de confidencialidad y el ejercicio personal de la función arbitral, pero, sobre todo, establecen un acercamiento al nivel de permisibilidad atribuido a la delegación de las funciones arbitrales.

El Centro de Arbitraje y Mediación de Silicon Valley (SVAMC) emitió las “*Guidelines on the Use of Artificial Intelligence in Arbitration*” (Abril 2024). La sección 3 contiene los lineamientos para árbitros:

Directriz 6

No delegación de responsabilidades en la toma de decisiones

Un árbitro no podrá delegar ninguna parte de su mandato personal en ninguna herramienta de IA. Este principio se aplicará especialmente al proceso de toma de decisiones del árbitro. El uso de herramientas de IA por parte de los árbitros no sustituirá su análisis independiente de los hechos, la ley y las pruebas (traducción libre).

Se refuerza una vez más el carácter personalísimo de la función arbitral y, al igual que el caso Yukos y el que resolvió la *Cour de Cassation* belga, la distinción se encuentra en una potencial injerencia en el *decision-making process*.

Asimismo, se establecen escenarios en donde la función indiscutiblemente recae en el árbitro: análisis de los hechos, las normas y las pruebas. Esto distinto de otros lineamientos y es de suma relevancia dado que justamente ese análisis es el que permite al árbitro dilucidar qué alegaciones son las acertadas. Serán la base para su construcción argumentativa. Si lo hace una IA, se pierde este pilar esencial en la toma de decisiones, no solamente por el efecto *black box*, sino también porque estas funciones son intrínsecamente humanas.

Los comentarios del SVAMC a aquella directriz también profundizan en ello:

Esta Directriz subraya el principio fundamental de que el mandato de un árbitro, especialmente su función última de toma de decisiones, es personal e indelegable. Esta Directriz no prohíbe ni restringe el uso de herramientas de IA por parte de los árbitros para ayudarles a cumplir con su responsabilidad y deber de analizar los hechos, los argumentos, las pruebas y la ley, y de emitir una decisión motivada (...).

Esta Directriz refuerza la necesidad de que los árbitros revisen los resultados generados por cualquier herramienta de IA para garantizar su exactitud y asuman toda la responsabilidad por cualquier error o inexactitud. Si un árbitro utiliza una herramienta de IA generativa para ayudarle en el análisis de los argumentos o en la redacción de cualquier parte de una decisión o laudo, el árbitro no puede limitarse a reproducir los resultados de la IA sin asegurarse de que reflejan adecuadamente su análisis personal e independiente de las cuestiones y pruebas que se le han presentado (...) (traducción libre) (pp. 19-20).

Se enfatiza entonces en que los árbitros tienen la obligación de hacer una revisión del contenido producido por la IA, tomando responsabilidad absoluta de cualquier error o inexactitud (p. 20). Por ejemplo, si determinada IA provee información sobre normas o jurisprudencia, es deber del árbitro corroborar que la misma exista y que sea precisa.

Asimismo, se establece que un árbitro puede usar IA para asistirse en el análisis de argumentos o borradores del laudo, pero si lo hace, “no puede simplemente reproducirmeramente imitar el texto emitido por la IA sin cerciorarse que refleja adecuadamente el análisis personal e independiente del árbitrosu juicio de los problemashechos y evidencia” (traducción libre, p. 20).derecho. Es decir, la IA puede redactar elsecciones del laudo, pero el árbitro debe corroborar que aquello plasma su razonamiento personal. Se sigue el mismo estándar que para los secretarios arbitrales: que la responsabilidad final recaiga en el árbitro.

Segundo, se encuentra la Directriz 7, Respeto del debido proceso, que establece lo siguiente:

Un árbitro no se basará en información generada por IA que no conste en el expediente sin informar previamente a las partes y, en la medida de lo posible, permitir que las partes presenten sus observaciones al respecto.

Cuando una herramienta de IA no pueda citar fuentes que puedan ser verificadas de forma independiente, el árbitro no asumirá que dichas fuentes existen o son caracterizadas con precisión por la herramienta de IA (traducción libre).

Es un estándar particular. A diferencia de lo sentado en el caso Yukos, en donde se afirmó que no informar a las partes sobre el rol del asistente en la elaboración del laudo no constituía una violación grave del mandato, aquí se establece una obligación para el árbitro de, no solamente informar a las partes el uso de información obtenida de IA, sino también que las partes puedan emitir sus comentarios, los cuales tendrá que considerar. Se consolida, de este modo, la transparencia y el derecho de las partes de ser escuchadas.

Resulta también interesante debido a que el escenario no necesariamente se repite en atención a los secretarios. Como observamos antes, los reglamentos arbitrales suelen considerar su participación, pero no es usual establecerlo en el convenio ni la necesidad de coordinarlo previamente con las partes. En cambio, al ser el uso de la IA un escenario novedoso e incipiente, resulta lógico que se disponga un deber de información.

Asimismo, establece la evidente obligación de no considerar fuentes no verificables emitidas por la IA. Como mencionan los comentarios: “It prompts arbitrators to evaluate the reliability of AI-derived information independently and critically” (p. 20), lo cual implica que el árbitro deberá asumir responsabilidad en contrastar la información y seleccionar lo comprobable.

Posteriormente, la Chartered Institute of Arbitrators (CI Arb) emitió su “*Guideline on the Use of AI in Arbitration (2025)*”³⁵, cuyo objetivo es guiar sobre el uso de IA para aprovechar sus beneficios y mitigar los riesgos a la integridad del proceso, los derechos de las partes o la aplicabilidad de cualquier laudo o *settlement agreement*. Se subraya que el árbitro sigue siendo plenamente responsable del laudo final, sin importar cualquier ayuda proporcionada por la IA. Él es el único responsable del resultado y no puede eludir su responsabilidad por error, inexactitud o violación de la confidencialidad.

En la sección “*Part IV: Use of AI by Arbitrators*” se establece lo siguiente en atención a la discrecionalidad sobre el uso de la IA por los árbitros:

- 8.2. Los árbitros no deben renunciar a su poder de decisión en favor de la IA, pero pueden utilizarla para apoyar un procesamiento más preciso y eficiente de la información presentada, garantizando siempre la independencia de criterio. Se aconseja a los árbitros que se abstengan de utilizar la IA de forma que pueda comprometer la integridad del procedimiento o la validez o ejecución del laudo. En concreto, el Tribunal debe evitar delegar tareas en las herramientas de IA, como el análisis jurídico, la investigación e interpretación de los hechos y el derecho, o la aplicación del derecho a los hechos, si dicho uso puede influir en las decisiones procesales o sustantivas.
- 8.3. Los árbitros también deben verificar de forma independiente la exactitud y corrección de la información obtenida a través de la IA, asegurándose de que su juicio está libre de sesgos de confirmación y otras distorsiones. Deben llevar a cabo su

35 Véase: https://www.ciarb.org/media/m5dl3pha/ciarb-guideline-on-the-use-of-ai-in-arbitration-2025-_final_march-2025.pdf

propia investigación, utilizando la información generada por la IA como herramienta de apoyo, manteniendo al mismo tiempo una perspectiva crítica para evitar influencias indebidas en sus decisiones, incluso mediante una supervisión adecuada.

- 8.4. Un árbitro asumirá la responsabilidad de todos los aspectos de un laudo, independientemente de cualquier uso de IA para ayudar en el proceso de toma de decisiones (traducción libre).

Este lineamiento es aún más concreto que el de la SVAMC. No solamente se enfatiza en que el poder de decisión debe mantenerse en la esfera del árbitro, sino también se incluyen entre las funciones inherentes: el análisis jurídico, investigación e interpretación de hechos y derecho, y aplicación del derecho. Aquello restringe de forma explícita las acciones que no le puede solicitar el árbitro a la IA.

Más aún, se establece que el árbitro debe realizar su propia investigación independiente, siendo que la información generada por la IA solamente es de apoyo, a diferencia del estándar de la SVAMC, donde el énfasis recae en la revisión del contenido que ya ha sido generado por la IA.

Por otro lado, se establece lo siguiente sobre la transparencia sobre el uso de la IA:

- 9.1. Salvo acuerdo en contrario de las partes, se insta a los árbitros a consultar con las partes sobre el uso de cualquier Herramienta de IA por parte de los árbitros y a ofrecer a las partes la oportunidad de comentar y oponerse al uso de dicha herramienta por parte de los árbitros. Si las partes no están de acuerdo sobre el uso de la IA por parte de los árbitros, éstos deberán abstenerse de utilizar la Herramienta de IA especificada. Cuando las partes estén de acuerdo sobre el uso específico de la IA por parte de los árbitros, se anima a los árbitros a tomar la decisión de proceder o no a la luz de todas las circunstancias del caso, incluidas las consideraciones detalladas en los párrafos 8.1 - 8.4 anteriores.
- 9.2. Un árbitro que forme parte de un Tribunal deberá consultar con los demás árbitros que formen parte del mismo Tribunal sobre el uso de cualquier Herramienta de IA en el contexto de su mandato (traducción libre).

Este lineamiento protege en gran medida a las partes del uso de la IA por parte del árbitro. Se establece, no solamente la obligación de consultar, sino también la posibilidad de que la parte se oponga y, en ese caso, la obligación del árbitro de abstenerse de usar IA (no previsto en los lineamientos SVAMC). Con ello, se protege plenamente la libertad de decisión de las partes, se salvaguarda el laudo de cualquier intromisión de la IA especificada como no utilizable y se promueve la transparencia de los árbitros.

Aunque todos estos instrumentos no son vinculantes por naturaleza, pues pertenecen al *soft law*, su autoridad e influencia en la práctica arbitral son indiscutibles. Esto se debe no solo a su asertividad, sino también a la precisión de su contenido. Se mantiene un estándar común: la IA es una herramienta, no un órgano decisorio. Su uso por parte de los árbitros no puede socavar la naturaleza *intuitu personae* de su función, ya que los árbitros siguen siendo, en última instancia, plenamente responsables del laudo dictado.

Cierto sector de la doctrina también ha considerado el establecimiento de una escala que evidencia los distintos usos de la IA en el proceso y la supervisión correspondiente que debe ejercer el tribunal, distinguiéndose entre: Minimal supervision (Level 1), Limited supervision (Level 2), Moderate supervision (Level 3), High supervision (Level 4) y Full supervision (Level 5)³⁶. Esta propuesta es particularmente significativa pues, no solo refleja la práctica arbitral actual, sino también identifica las funciones específicas que pueden delegarse a la IA y evalúa su potencial impacto en la integridad del proceso. Así, se proporciona a los árbitros una orientación práctica y sencilla de cómo integrar responsablemente la IA en su trabajo.

V. Conclusiones y recomendaciones

La inteligencia artificial es, sin duda alguna, uno de los avances tecnológicos de mayor trascendencia en la época contemporánea y otorgan innumerables beneficios en la práctica jurídica. No obstante, también se debe garantizar que su uso no trasgreda la integridad del proceso

³⁶ PAULSSON, M. & SURESH, S. (2024). AI The Modern Tribunal Assitant - Impact on Enforceability of Arbitral Awards under the New York Convention. *JusMundi Arbitration Review*, 1(1), 101-108.

arbitral. Y esto es de especial importancia debido a que ha comenzado a discutirse en sede judicial la validez de los laudos emitidos con asistencia de la IA, como en el caso *LaPaglia v. Valve Corporation* (2025).

Para evitar ello, deben establecerse límites nítidos a los tipos de funciones que pueden ser o no delegadas: distinguir visiblemente entre labores administrativas y adjudicativas. Aquellas reglas pueden ser implementadas por las mismas partes o consultadas por el árbitro con anterioridad. También es conveniente el disclosure arbitral en atención al uso de IA. Finalmente, los árbitros deberán considerar los estándares internacionales incipientes en materia de IA y proceso arbitral y, de forma subsidiaria, los establecidos previamente en razón de la asistencia de terceros en el arbitraje.

En este marco, existe un estándar mínimo, imperativo e inobjetable: el proceso de toma de decisión, en ninguna circunstancia, puede delegarse a la IA. Y, en caso de existir algún escenario impreciso o gris, el control humano debe mantenerse, asegurando la autoría y responsabilidad final sobre el laudo. Como bien señalaron los profesores Redfern y Hunter en atención a la asistencia de terceros: “el objetivo es asistir al tribunal arbitral, no usurpar su función”³⁷.

³⁷ REDFERN y HUNTER, op. cit., p. 301.

La economía digital y el derecho a monetizar la información: Un camino posible

Octavio Salazar Mesías*

Resumen.- El presente artículo analiza los desafíos que la economía digital plantea a la tributación internacional y propone como alternativa el reconocimiento del derecho a monetizar los datos personales (DMDP). Se plantea la creación de un Identificador Tributario Digital Único (ITDU) y un sistema de reporte digital que traslade la carga tributaria a las MNEs, garantizando transparencia, equidad fiscal y reconocimiento de los derechos de las jurisdicciones de mercado.

Palabras clave.- Tributación Internacional – Datos Personales – Monetización de Información – Fiscalización Tributaria Digital – Herramientas Legales Digitales.

Abstract.- This article analyzes the challenges that the digital economy poses to international taxation and proposes, as an alternative, the recognition of the right to monetize personal data. It proposes the creation of a Unique Digital Tax Identifier and a digital reporting system that shifts the tax burden to MNEs, ensuring transparency, tax fairness, and recognition of the rights of market jurisdictions.

Keywords.- International Taxation – Personal Data – Monetization of Information – Digital Tax Auditing – Digital Legal Tools.

* Sobre el autor: Socio de Ecovis Perú. Abogado por la Pontificia Universidad Católica del Perú (PUCP), postgrado en Derecho Tributario Internacional en la Universidad Austral de Buenos Aires (Argentina) y el International Tax Center de la Universidad de Leiden (Holanda); y LL.M. en International Tax Law por la Universidad de Negocios y Economía de Viena (Wirtschaftsuniversität Wien). Miembro del Instituto Peruano de Derecho Tributario y de la Asociación Fiscal Internacional - Grupo Peruano.

I. Introducción

En el mundo digital actual, la información se ha transformado en uno de los activos más preciados por parte de los actores económicos¹. Grandes corporaciones tecnológicas han edificado auténticos imperios basados en la recopilación, procesamiento y comercialización de los datos de las personas. No obstante, quienes generan estos datos (los usuarios) casi nunca reciben una retribución por el uso comercial de su información privada.

La realidad ha creado complejos problemas fiscales² en el mundo entero. Gigantes como Google, Meta (Facebook), Amazon y otras operan con esquemas comerciales que requieren un flujo constante de datos aportados por sus usuarios, y pueden obtener enormes ganancias en territorios donde no cuentan con instalaciones físicas, lo que complica la implementación de los convencionales criterios de gravamen internacionales.

Precisamente, con el fin de abordar los desafíos planteados por la tributación de la economía digital, donde resalta la obsolescencia de los actuales sistemas de tributación vigentes en el mundo, la Organización para la Cooperación y el Desarrollo Económicos (OCDE)³ y el Grupo de los Veinte (G20) han propuesto una solución enfocada en dos pilares. El Pilar Uno consiste en crear un nuevo vínculo fiscal para las empresas multinacionales (EMN), donde la falta de presencia física no sea un impedimento para que una jurisdicción grave los ingresos de dichas entidades⁴.

¹ Customer Data Platform Institute. (21 de abril de 2023). El valor de los datos de los clientes: ¿cuánto podrían valer? Recuperado de: <https://www.abc.es/economia/hacienda-maniobra-gravar-youtubers-exiliados-andorra-eventos>.

² Organización para la Cooperación y el Desarrollo Económicos [OCDE]. (2021). Declaración sobre el enfoque de dos pilares para abordar los desafíos fiscales derivados de la digitalización de la economía. <https://www.oecd.org/tax/beps/declaracion-sobre-el-enfoque-de-dos-pilares-para-abordar-los-desafios-fiscales-derivados-de-la-digitalizacion-de-la-economia-octubre-2021.pdf>.

³ Organización para la Cooperación y el Desarrollo Económicos [OCDE]. (2024). Base Erosion and Profit Shifting Project: Pillar One – Amount B. https://www.oecd-ilibrary.org/taxation/pillar-one-amount-b_21ea168b-en

⁴ Organización para la Cooperación y el Desarrollo Económicos [OCDE]. (2021). Declaración sobre el enfoque de dos pilares para abordar los desafíos fiscales derivados de la digitalización de la economía. <https://www.oecd.org/tax/beps/declaracion-sobre-el-enfoque-de-dos-pilares-para-abordar-los-desafios-fiscales-derivados-de-la-digitalizacion-de-la-economia-octubre-2021.pdf>.

Recordemos que la estructura del actual régimen de tributación internacional se remonta a los años 1920 y siguientes, una época en la que la economía del comercio internacional se basaba netamente en artículos tangibles y la comunicación entre los protagonistas era lenta⁵. Como resultado de ello, la tributación doméstica se ha construido bajo el denominado principio de territorialidad, basándose tanto en el contribuyente, según su residencia fiscal, como en el vínculo geográfico con el hecho imponible, entendido como la fuente de ingresos⁶.

El principio básico reinante en el mundo es precisamente el de territorialidad⁷; y bajo dicha guía se han generado problemas en términos de doble tributación internacional o el múltiple gravamen. En efecto, buscando mitigar aquella situación y armonizar la fiscalidad internacional, se ha avanzado en la celebración de tratados internacionales como los convenios para evitar la doble imposición, cuyo estándar radica en los modelos aprobados por la OCDE. Estos cuerpos legales suelen dar importancia a la presencia física de los no residentes, gravando principalmente según el estado de residencia, a menos que haya un establecimiento permanente en el otro estado⁸.

[org/tax/beps/declaracion-sobre-el-enfoque-de-dos-pilares-para-abordar-los-desafios-fiscales-derivados-de-la-digitalizacion-de-la-economia-octubre-2021.pdf](#)

- ⁵ KOBETSKY, M. (2011). Historia de los tratados fiscales y el concepto de establecimiento permanente. En *Tributación internacional de establecimientos permanentes: Principios y políticas* (Cambridge Tax Law Series). Cambridge University Press.
- ⁶ GADZO, S. (2018). The principle of 'nexus' or 'genuine link' as a keystone of international income tax law: A reappraisal. *Intertax*, 46(3), 194–209.
- ⁷ KOKOTT, J. (2022). Derecho Internacional Público y Tributación: Nexo y territorialidad. En E. Traversa (Ed.), *Nexo Fiscal y Jurisdicción en el Derecho Internacional y de la UE*, pp. 5.
- ⁸ DANTAS, E. (2022). Desafíos fiscales de la economía digital: una evaluación de la nueva regla de nexos de la OCDE basada en umbrales de ingresos. *Boletín de Tributación Internacional*, pp 3.

En estos tiempos, y por diversos factores⁹, una parte importante de la economía se ha digitalizado por completo, lo que no solo implica el auge de nuevos modelos de negocios, sino también mercados y productos digitales. De esta manera, el proceso de creación de valor ha evolucionado significativamente para las EMN. Consecuentemente, la tendencia de mantener instalaciones físicas disminuirá con el tiempo hasta el punto en que no será necesaria ninguna presencia física, y las actividades se realizarán especialmente de forma remota¹⁰.

Bajo este contexto, y como respuesta a la situación planteada anteriormente, diferentes países vienen reformulando sus conceptos de territorialidad para incluir la economía digital, creando múltiples nexos aplicables. Con esto, además, se viene acentuando la necesidad de coordinar las jurisdicciones superpuestas de estos países y abordar la complejidad generada por tener múltiples ordenamientos de tributación que naturalmente podrían colisionar.

Hasta la fecha, si bien una de las soluciones internacionales más prometedoras a la problemática de la tributación internacional sería la propuesta diseñada en el Pilar Uno de la OCDE, la cual –junto con el Pilar Dos– introduce nuevos instrumentos de asignación que se utilizarán además del método existente para compensar las deficiencias del modelo tributario internacional, mediante el presente trabajo de investigación no solo revisaremos el tema en cuestión, sino que quisiéramos además plantear una alternativa distinta: el derecho a monetizar los datos personales (“DMDP”).

Lo antes expuesto se basa en la premisa de que las personas deberían obtener un pago económico por parte de las compañías que utilizan

⁹ Según el reporte estadístico Instituto Nacional de Salud y Centro Nacional de Epidemiología, Prevención y Control de Enfermedades (2021), el Perú ha sido uno de los países más afectados por este virus en toda la región. Esto, a su vez, aceleró una creciente evolución normativa relacionada con el teletrabajo. Precisamente, en mayo de 2023, el Ministerio de Trabajo y Promoción del Empleo (MTPE) informó que más de 220,000 personas realizaban teletrabajo en el país, siendo esta una medida aplicable tanto en el sector privado como en el público.

¹⁰ Organización para la Cooperación y el Desarrollo Económicos [OCDE]. (2019). Propuesta de la Secretaría para un “Enfoque Unificado” bajo el Pilar Uno: Documento de consulta pública (9 de octubre–12 de noviembre de 2019). Publicaciones de la OCDE.

su información personal; esto se conoce como el DMDP. En ese orden, el presente estudio se centra en responder la siguiente cuestión: ¿qué obstáculos impositivos enfrentan los individuos al ejercer su derecho a generar ingresos a partir de sus datos, y de qué manera se puede facilitar la fiscalidad de las ganancias obtenidas por este concepto? Para responder las interrogantes, la investigación pretende aprovechar los avances tecnológicos para diseñar un mecanismo de cooperación internacional que garantice una imposición eficiente del DMDP en el entorno digital, aportando así nuevas perspectivas a la discusión global sobre la regulación fiscal en la era tecnológica.

II. Breve aproximación al Pilar Uno

En los términos de la OCDE, la consigna del Pilar Uno es asegurar una distribución más equitativa de los beneficios y los derechos de imposición entre los países, especialmente en el caso de las EMN que son las máximas beneficiarias de la globalización¹¹. Dentro de este contexto, el Pilar Uno busca ampliar los derechos de imposición de las jurisdicciones de mercado (que, para algunos modelos de negocios, son las jurisdicciones donde los usuarios están físicamente ubicados), siempre que exista una participación activa y sostenida de un negocio en esa economía específica a través de actividades dirigidas de manera presencial o remota hacia esa jurisdicción en particular¹².

Concretamente, el Pilar Uno se aplicará inicialmente a las EMN con un volumen de negocios global superior a los 20 mil millones de euros y una rentabilidad superior al 10% (i.e., beneficio antes de impuestos/ Ingresos). Cuando la EMN obtenga al menos 1 millón de euros en ingresos de una jurisdicción de mercado, se asignará un determinado importe sobre esa jurisdicción de mercado, la cual podrá gravar. El

¹¹ Organización para la Cooperación y el Desarrollo Económicos [OCDE]. (2021). Puntos destacados: Enfoque de dos pilares para abordar los desafíos fiscales derivados de la digitalización de la economía (Octubre 2021). OCDE. Recuperado de: <https://www.oecd.org/tax/beps/puntos-destacados-enfoque-de-dos-pilares-para-abordar-los-desafios-fiscales-derivados-de-la-digitalizacion-de-la-economia-octubre-2021.pdf>

¹² Organización para la Cooperación y el Desarrollo Económicos [OCDE]. (2020). Tax Challenges Arising from Digitalisation – Report on Pillar One Blueprint: Inclusive Framework on BEPS, pp. 11.

umbral de ingresos se reducirá para jurisdicciones más pequeñas (PIB < 40 mil millones de euros) a 250,000 euros.

Así pues, cuando sea aplicable, el 25% de las ganancias residuales (más del 10% de los ingresos) de la EMN se asignará a la jurisdicción de mercado mediante un criterio de asignación basado en los ingresos. En esencia, el Pilar Uno supone un cambio radical al concepto actual incluido en la mayoría de los tratados fiscales, que requiere la existencia de un establecimiento permanente en una jurisdicción antes de que surja el derecho a gravar las ganancias de una empresa. En cambio, la imposición se asentará en el uso o consumo de bienes o servicios dentro de la jurisdicción de mercado.

Importante resaltar que el Pilar Uno está estructurado en términos de “Monto A”, por un lado, y “Monto B”, por otro. En cuanto al Monto A, se centra en apartar parte de las ganancias residuales de las empresas más grandes y rentables del mundo en beneficio de las jurisdicciones en las que se suministran bienes o servicios o donde se encuentran los clientes (jurisdicciones de mercado)¹³.

El Monto A contempla un nuevo derecho impositivo para las jurisdicciones de mercado sobre una porción de las ganancias residuales que, a su vez, se evalúa a nivel del grupo de EMN (o segmento, línea de negocios, etc.)¹⁴. De otra parte, el Monto B se enfoca en simplificar la aplicación del principio de plena competencia (“ALP”, por sus siglas en inglés), lográndolo al determinar las ganancias atribuibles a actividades de marketing y distribución, así como mejorando la certeza tributaria mediante la cooperación tributaria multilateral¹⁵.

¹³ Organización para la Cooperación y el Desarrollo Económicos [OECD]. (2022). Public Consultation Document – Progress Report on Amount A of Pillar One: Two-Pillar Solution to the Tax Challenges of the Digitalisation of the Economy, 11 July – 19 August 2022, pp. 8.

¹⁴ ADDA, M., SCANDONE, F. S., & LORENZI, U. (2021). The new taxing right under Pillar One: Preliminary thoughts on potential implications for MNEs. *International Transfer Pricing Journal*, 28(1), pp. 10

¹⁵ VAN DAM, H., KIÈS, C., KLETHI, P.A., VAN DER KROON, S., KUNEN, J.W., & DA SILVA, B. (2021). Taxing the digitalized economy: Key takeaways from the OECD public consultation on the Pillar One and Pillar Two blueprints. *International Transfer Pricing Journal*, 28(3), pp. 165.

Fluye de lo expuesto que se deben cumplir dos umbrales para que un grupo cubierto –EMN y en general todas las entidades económicamente vinculadas– sea considerado como sujeto a los términos del Pilar Uno. El primer umbral tiene en cuenta el monto mínimo de ingresos del grupo (i.e., la prueba de los ingresos globales), que es una cantidad establecida con un volumen de negocios anual global superior a los 20 mil millones de euros. El segundo umbral, por su parte, aborda los márgenes de beneficio de la EMN (i.e., la prueba de rentabilidad), estableciendo el límite para las EMN con un margen de beneficio superior al 10 % (beneficio antes de impuestos/ingresos). Por lo tanto, las EMN con ingresos inferiores a los 20 mil millones de euros en el período actual, así como las empresas con pérdidas o aquellas con márgenes de beneficio bajos, quedan excluidas del alcance.

Nótese que, con la emisión del Pilar One – Amount B, aprobado por el Marco Inclusivo de la OCDE/G20 sobre BEPS (sujeto a reservas registradas por parte de India), las empresas deberán evaluar si tienen transacciones que puedan estar dentro del alcance del Monto B y, con ello, estimar el impacto financiero en su operación. Precisamente, será importante para las empresas monitorear la implementación del aludido Monto B por parte de las jurisdicciones en donde lleven a cabo negocios¹⁶.

De la misma forma, las fechas de implementación por parte de las jurisdicciones relevantes deben ser monitoreadas ya que esto podría ser relevante para contabilizar el impacto fiscal y, consecuentemente, la tasa impositiva efectiva del grupo¹⁷. Además, el documento se incorpora en las Directrices de la OCDE sobre Precios de Transferencia como un Anexo al Capítulo IV.

Ahora bien, las posiciones y opiniones relacionadas al Pilar Uno son diversas. Algunos, por ejemplo, plantean iniciar la implementación del Pilar Uno con un escalón de alcance más elevado. De ese modo, únicamente las EMN más grandes y rentables serán sometidas al régimen, reduciendo gradualmente los trancos a lo largo de los años e incrementando progresivamente el número de entidades incluidas en

¹⁶ Ernst & Young [EY]. (2024). OECD releases final guidance on Pillar One – Amount B. Ernst & Young. Recuperado de: https://www.ey.com/en_be/tax/tax-alerts/2024/oecd-releases-final-guidance-on-pillar-one-amount-b

¹⁷ *Ibidem*.

el rango establecido. Esto, además, sugiere la posibilidad de eficiencia en cuanto a los costos de implementación por parte de las autoridades tributarias. Otra opción es comenzar a reducir los umbrales solo después de que haya transcurrido un período de revisión¹⁸.

En este sentido, dependiendo del éxito del uso del Monto A, y contemplando la esfera de la certeza tributaria deseada (i.e., sustentada en el principio de seguridad jurídica¹⁹), el volumen de negocios anual total para que una gran empresa entre en el ámbito del Monto A disminuirá de 20 a 10 mil millones de euros. La revisión previamente mencionada está programada para llevarse a cabo siete años después de la entrada en vigor del acuerdo. Conjuntamente, deberá completarse en un plazo máximo de un año calendario²⁰.

Cabe destacar que las reglas del Pilar Uno, en mayor o menor medida, continúan abiertas. Esto es, aún no han sido completamente desarrolladas y, conforme lo hemos mencionado, es previsible esperar cambios en su desarrollo. Nótese, de cualquier modo, que aunque las pautas puedan ser rediseñadas, persistirán los desafíos de implementación, así como otras cuestiones que –bajo nuestra vista– tendrían que repotenciarse.

III. Incertidumbres sobre el Pilar Uno y temas por evaluar

Es claro que el Pilar Uno requerirá de esfuerzos conjuntos para su implementación y no se trata de una herramienta autoejecutable. Por lo tanto, una de las principales complejidades presentadas es la necesidad de “domesticar” o incorporar la norma fiscal internacional para

¹⁸ Organización para la Cooperación y el Desarrollo Económicos [OCDE]. (2020). *Tax Challenges Arising from Digitalisation – Report on Pillar One Blueprint: Inclusive Framework on BEPS*. OECD Publishing.

¹⁹ Si bien nuestro ordenamiento no se remite de modo expreso al concepto de seguridad jurídica¹³³; el Tribunal Constitucional se refiere a este como un pilar consubstancial del Estado Constitucional de Derecho, principio constitucional, relacionándolo con la predictibilidad de las conductas (en especial, la de los poderes públicos) frente a los supuestos previamente determinados por el Derecho, señalando que la seguridad jurídica “es la garantía que informa a todo el ordenamiento jurídico y que consolida la interdicción de la arbitrariedad”. Sentencia del Tribunal Constitucional de fecha 30 de abril de 2003, recaída en el Expediente No. 0016-2002-AI/TC.

²⁰ Organización para la Cooperación y el Desarrollo Económicos [OECD]. (2021). *Addressing the Tax Challenges of the Digitalisation of the Economy*.

que pueda aplicarse dentro de una jurisdicción determinada. Esto, principalmente, se puede hacer mediante reglas internas o a través de una convención multilateral²¹.

Conviene tener presente que, en octubre de 2023, el TFDE publicó un texto del Convenio Multilateral (CM), junto con su declaración explicativa y el entendimiento sobre la ‘Aplicación de la Certeza’ para el Monto A del Pilar Uno, que reflejaba el consenso alcanzado hasta ese momento entre los miembros sobre la arquitectura técnica del referido Monto A. El objetivo de dicho documento fue garantizar la transparencia, facilitar la capacidad de algunos miembros para participar en procesos internos requeridos para adaptarse exitosamente a lo dispuesto por el TFDE y facilitar la resolución de las diferencias pendientes²².

En estricto, resolver las diferencias es un trabajo que continúa en realización, además del estancamiento en los nuevos impuestos sobre servicios digitales y otras medidas similares relevantes. Por lo tanto, el compromiso del TFDE sigue vigente y se espera finalizar el texto del MLC los miembros del Marco Inclusivo reafirman su compromiso de lograr una solución basada en el consenso y finalizar el texto del CM en marzo de 2024.

A la luz de otros antecedentes tratándose también de iniciativas OCDE, se espera que los países lleguen a un acuerdo, seguido de la firma de una convención para la puesta en marcha del Pilar Uno. Sin embargo, algunos autores creen que quizás sea demasiado optimista esperar que las leyes fiscales nacionales divergentes puedan integrarse para abordar los desafíos de la globalización digital²³.

Respecto del caso peruano, la complejidad de implementar el Pilar Uno puede ser mayor para los países en desarrollo debido a la falta de capacidad para llevar a cabo reformas, puesto que puede no ser una prioridad y hay una experiencia limitada disponible. Es aún más

²¹ LI, J. (2021). The legal challenges of creating a global tax regime with the OECD Pillar One Blueprint. *Bulletin for International Taxation*, 75(2), pp. 84-93.

²² Organización para la Cooperación y el Desarrollo Económicos [OECD]. (2023). Update to Pillar One timeline by the OECD/G20 Inclusive Framework on BEPS.

²³ LI, op. cit., pp. 93.

complejo cuando se tiene en cuenta el tiempo limitado asignado para la implementación de la medida²⁴.

De ese modo, aun cuando el Perú ha sido uno de los países socios más activos en comprometerse con la OCDE y la adopción de sus instrumentos, todavía no somos un país miembro. Consecuentemente, el Pilar Uno podría estar aún más lejos²⁵ para nosotros que para otros vecinos de la región; ello sin mencionar la coyuntura política y económica (con desafortunados indicadores como los altos niveles de informalidad y la reciente recesión) que nos acompaña.

Considerando estos argumentos, sería válido encontrar cierto especismo entre la mayoría de actores en cuanto a la eficacia del Pilar Uno. Propiamente, la “solución final” para la tributación de la economía actual (que está compuesta por empresas con presencia física, presencia digital o ambas) aún tiene trabajo pendiente.

Además, las EMN que actualmente pagan impuestos normalmente bajo las reglas actuales advertirán que dichas reglas coexisten con los nuevos impuestos propuestos, generando –cual tratándose de un canon– mayores costos administrativos o conflictos entre los dos sistemas, no solo para los contribuyentes sino también para las autoridades fiscales²⁶.

Otra cuestión discutible es la referida a las reglas del nexo y los umbrales del PIB. Por ejemplo, si un grupo cubierto obtiene 1 millón de euros en ingresos dentro de una jurisdicción, la misma sería elegible para el Monto. No obstante, si el producto interno bruto de la jurisdicción es inferior a 40 mil millones de euros, el umbral se reducirá a 250,000 euros.

El compromiso del umbral, entonces, sea éste en 1 millón de euros o en 250,000 euros, ha sido objeto de discusión, puesto que el PIB no es un indicador estable a lo largo del tiempo, sino que puede variar año tras

²⁴ LI, op. cit., pp. 94.

²⁵ International Monetary Fund. (2023). International corporate tax reform (Policy Paper No. 2023/001, pp. 19). International Monetary Fund.

²⁶ LI, op. cit., pp. 87.

año²⁷. Ello, precisamente, podría afectar la certeza fiscal para las EMN que obtienen ingresos cercanos a los rangos establecidos.

Ante lo anterior, una propuesta es que los umbrales de PIB establecidos permanezcan vigentes durante un período de tiempo más prolongado, al menos hasta el inicio de la implementación del Monto A²⁸; o, alternativamente, que la OCDE, con determinada periodicidad, publique una lista de países que cumplen con los estándares de PIB para garantizar la coherencia en su ejercicio a nivel general. También se ha destacado la necesidad de especificar –con el sustento debido, claro– las razones económicas detrás de cualquiera de las opciones de política preferidas.

La determinación del monto del PIB es relevante, dado que cuanto mayor sea el umbral del PIB, menos jurisdicciones serán elegibles para la asignación del Monto A, y si el monto de los ingresos es menor, más jurisdicciones serían elegibles. Lo dicho, ciertamente, plantea argumentos a favor o en contra de aumentar o disminuir los umbrales, dependiendo de la propuesta.

Tan solo aquellos países que generan grandes ingresos dentro de una jurisdicción de mercado se benefician con la asignación del Monto A, al reducir los costos y esfuerzos administrativos necesarios para el cumplimiento tanto de las autoridades fiscales como de los contribuyentes. Por el contrario, se podría argumentar que la reducción de los umbrales del PIB permitiría a los países beneficiarse de esta medida al generarse mayores ingresos, lo que sucedería eventualmente en el caso peruano y otros estados de la región.

Con relación al Monto B, entre los temas pendientes se encuentra la definición o modelo del acuerdo que tendrían que adoptar las autoridades competentes, y que se utilizarían en el contexto de jurisdicciones de baja capacidad y relaciones bilaterales donde el objeto sea evitar la

²⁷ BARBOSA, M. H., & PETRUZZI, R. (2022). Comments to the Public Consultation Document ‘Pillar One – Amount A: Draft Model Rules for Nexus and Revenue Sourcing’ (OECD public consultation). OECD.

²⁸ VAN DAM, H., VÁZQUEZ, J. M., BURIK, S., & KUNEN, J.W. (2022). Comments to the Public Consultation – Progress Report on Amount A of Pillar One. Loyens & Loeff.

doble imposición, pero también prevenir la doble no imposición. Esto, se advierte, sería desarrollado en el Inclusive Framework durante el 2024.

Por último, la complejidad del Pilar Uno y su implementación sería muy marcada para los países en desarrollo, debido principalmente a la falta de capacidad para llevar a cabo reformas. En estricto, nuestra experiencia reciente comprueba que, cuando los temas en agenda no son prioridades para los grupos políticos que ostentan el poder, el avance es limitado, por no decir nulo. El tema se vuelve más complejo cuando notamos la presencia de períodos (definidos) que serán asignados para implementar la medida²⁹.

IV. Una propuesta de cambio: Monetización de la información y DMDP

i. El valor de la información y la relación triangular

A diferencia de los activos tangibles, cuya naturaleza impide su fraccionamiento o distribución simultánea, los activos digitales presentan una característica única: pueden copiarse, multiplicarse y compartirse entre diversos actores al mismo tiempo sin perder su integridad original³⁰. Esta cualidad ha abierto la puerta a modelos de negocio capaces de generar valor de manera exponencial. Con esa lógica, las empresas han encontrado dos vías principales para rentabilizar los datos personales: una directa, mediante su comercialización con terceros, y otra indirecta, al transformar esos datos en insumos que permiten desarrollar nuevos productos, servicios o información de valor agregado, que luego son comercializados en el mercado³¹.

La transformación digital está cambiando profundamente el mundo, alterando cómo las empresas interactúan con sus clientes y cómo los

²⁹ International Monetary Fund. (2023). International corporate tax reform (Policy Paper No. 2023/001), pp. 19.

³⁰ EY Global. (2018). How to monetize IoT data to create value. Ernst & Young Global Ltd. Recuperado de: https://www.ey.com/en_gl/consulting/how-to-monetize-iot-data-to-create-value.

³¹ FRED, J. (2017). Data monetization – How an organization can generate revenue with data? [Tesis de maestría, Tampere University of Technology]. Tampere University of Technology.

individuos interactúan entre sí. Los datos son el eje de esta economía digital, y su valor comercial se ha convertido en una importante fuente de ingresos para muchas empresas tecnológicas³². En este contexto, la monetización de datos se ha convertido en una práctica común: las empresas recopilan datos personales de los usuarios, los analizan y los convierten en información procesable que puede ser vendida o utilizada para dirigir anuncios u optimizar servicios, programar campañas de ventas, entre otros³³.

El fenómeno descrito es resultado directo del aprovechamiento masivo de técnicas de minería de datos y de procesos de monetización de información digital³⁴. Este último consiste en transformar grandes volúmenes de datos corporativos (habitualmente sin estructura y subutilizados) en activos informacionales valiosos, susceptibles de ser convertidos en ingresos, ya sea mediante pagos directos o como contraprestación de servicios³⁵.

Lejos de limitarse a la venta de bases de datos crudas o tratadas, la monetización de datos engloba estrategias más complejas. Las organizaciones los emplean como insumo para desarrollar productos orientados al valor, generar rendimientos financieros, y obtener beneficios económicos indirectos como descuentos comerciales, campañas publicitarias financiadas por terceros, o incluso reducción de costos operativos derivados de una mayor eficiencia basada en analítica³⁶.

Este modelo de explotación ha generado un crecimiento sostenido a nivel global. De hecho, se estima que el mercado internacional de monetización de datos, valorado en 2.100 millones de dólares en 2020, superará los 15.400 millones de dólares para el año 2030, con una

³² EY Global, op. cit.

³³ FRED, op. cit.

³⁴ KANHAIYA, K., PRADEEP, R., & VINEET, K. (2022). Data monetization market research, 2030. Allied Market Research. Recuperado de: <https://www.alliedmarketresearch.com/data-monetization-market>.

³⁵ *Ibidem*.

³⁶ OFULUE, J., & BENYUCEF, M. (2022). Data monetization: Insights from a technology-enabled literature review and research agenda. *Management Review Quarterly*, 74(2), pp. 521-565. Springer.

tasa de crecimiento anual compuesta del 22,1 % durante el período 2021-2030³⁷.

Ahora bien, la relación entre los usuarios, las empresas digitales y los anunciantes se ha vuelto cada vez más compleja y entrelazada en la era de la monetización de datos. Existe una doble carga para los usuarios, quienes, al ceder sus datos personales, no solo renuncian a su privacidad, sino que además son objeto de publicidad dirigida, la cual puede resultar intrusiva e incluso percibirse como injusta, al generar una sensación constante de vigilancia.

En consecuencia, a medida que las empresas digitales continúan obteniendo beneficios económicos a partir de la utilización o comercialización de los datos personales, surge una interrogante fundamental: ¿los beneficios que reciben los consumidores (como el acceso a redes sociales o la funcionalidad de búsquedas predictivas) guardan proporcionalidad con el valor económico de los datos que se extraen de ellos?³⁸

ii. DMDP: Una revisión conceptual

En este contexto, diversos académicos han venido promoviendo la teoría del “dato como trabajo” (“data as labour theory”), la cual sostiene que los usuarios deben ser considerados no como proveedores de capital, sino como proveedores de trabajo, y que, por ende, deben tener derecho a una remuneración por su contribución^{39 40}. Autores como Jaron Lanier y E. Glen Weyl han desarrollado el concepto de “dignidad de los datos” (“data dignity”), y argumentan que los datos constituyen una forma

³⁷ Agencia de la Unión Europea para la Ciberseguridad [ENISA]. (2018). The Value of Personal Online Data. ENISA. Recuperado de: <https://www.enisa.europa.eu/publications/info-notes/the-value-of-personal-online-data>

³⁸ FRED, op. cit.

³⁹ ARRIETA, I., GOFF, L., JIMENEZ, D., LANIER, J., & WEYL, E. G. (2018). Should we treat data as labor? Moving beyond “free.” American Economic Association Papers and Proceedings, 108, pp. 38-42.

⁴⁰ HARRIS, R. (2020). Forging a path towards meaningful digital privacy: Data monetization and the CCPA. Loyola of Los Angeles Law Review, 53(1), pp. 223-250.

de trabajo, por lo que su apropiación sin compensación constituye una forma de explotación laboral⁴¹.

Para hacer posible el reconocimiento de la dignidad de los datos, en algunas jurisdicciones se están realizando esfuerzos por reforzar los derechos de propiedad sobre los datos personales⁴². Andrew Yang, ex candidato presidencial de Estados Unidos, ha propuesto que los individuos deben tener propiedad legal sobre sus datos personales, y que estos deben ser tratados como un bien patrimonial⁴³. Yang sostiene que actualmente las personas no reciben una compensación adecuada por el valor de sus datos, lo que les niega autonomía y dignidad sobre su información personal⁴⁴.

Esta línea de pensamiento también ha ganado tracción en la política europea⁴⁵ y canadiense⁴⁶. La ex canciller alemana Angela Merkel, por

⁴¹ LANIER, J., & WEYL, E. G. (2018). A blueprint for a better digital society. *Harvard Business Review*, 96(5), pp. 128-137.

⁴² "For example, the 2019 Own Your Own Data Act [in the US] attempted to provide people with property rights over their data, [by] developing a licensing system that focused on portability" Own Your Own Data Act, S. 806, 116th Cong. (as introduced by Sen. John Kennedy, 14 March 2019); COFONE, I. N. (2021). Beyond data ownership. *Cardozo Law Review*, 43(2), pp. 507-553.

⁴³ SWANT, M. (2019). Andrew Yang proposes digital data should be treated like a property right. *Forbes*. Recuperado de: <https://www.forbes.com/sites/martyswant/2019/11/01/andrew-yang-proposes-digital-data-should-be-treated-like-a-property-right>

⁴⁴ YANG2020. (2019). Regulating technology firms in the 21st century. Recuperado el 1 de abril de 2025, de <https://2020.yang2020.com/blog/regulating-technology-firms-inthe-21st-century>.

⁴⁵ "The European Commission launched a consultation group assessing data ownership"; Comisión Europea. (2014). Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Towards a thriving data-driven economy (COM/2014/0442 final). Recuperado de: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52014DC0442>.

⁴⁶ "The Canadian government Committee on Access to Information, Privacy, and Ethics has recommended establishing rules and guidelines regarding data ownership and data sovereignty with the objective of ending the non-consented collection and use of citizens' personal information" Zimmer, B. (2018). Addressing digital privacy vulnerabilities and potential threats to Canada's democratic electoral process. House of Commons of Canada; COFONE, op. cit.

ejemplo, ha defendido la necesidad de una regulación uniforme a nivel de la Unión Europea que establezca un marco común sobre la titularidad de los datos para estos fines comerciales⁴⁷. Propuestas similares han sido presentadas por distintos grupos mediáticos y por miembros de la comunidad de desarrolladores de blockchain, quienes consideran que esta tecnología puede ser instrumental para restituir a los usuarios el control sobre sus datos⁴⁸. En esa misma línea, Isabella de Michelis y Luca Bolognini, en su ensayo titulado “Una introducción al derecho a monetizar”, sostienen que los usuarios deben tener un papel más activo en los procesos de minería de datos y elaboración de perfiles, y que debe garantizarse una compensación justa por el uso de sus datos personales⁴⁹. Proponen la creación de un marco jurídico que permita a los usuarios finales transferir sus datos personales (incluidos aquellos generados por dispositivos del Internet de las Cosas) bajo un régimen de derechos de propiedad⁵⁰.

Permitir que los usuarios participen directamente en la creación de valor digital generaría economías de escala y fomentaría una competencia más saludable en el mercado. En conclusión, De Michelis y Bolognini afirman que, en el entorno digital (donde los datos de los usuarios constituyen la materia prima para el desarrollo de productos y servicios digitales) resulta injusto excluir a los propios usuarios de las oportunidades de monetización de esos datos⁵¹. Por ello, abogan por un nuevo marco normativo que otorgue a los usuarios de Internet el “derecho a monetizar”.

⁴⁷ Ver la Conferencia de Prensa. Merkel: Regulate Ownership of Data (2017). Consulta: 17 de abril de 2025, <https://www.bundesregierung.de/bregde/aktuelles/merkel-eigentum-an-daten-regeln-745810>. COFONE, op. cit.

⁴⁸ Por ejemplo. “The Financial Times” argumentó en 2018 que los consumidores deberían recibir compensaciones por permitir la utilización de sus datos; Financial Times. (2018, marzo 21). Data privacy rights require data ownership. Recuperado el 28 de marzo de 2025, de <https://www.ft.com/content/a00ecf9e-2d03-11e8-a34a-7e7563b0b0f4>

⁴⁹ DE MICHELIS, I., & BOLOGNINI, L. (2018). An introduction to the right to monetize (RTM). Istituto Italiano per la Privacy e la Valorizzazione dei Dati..

⁵⁰ *Ibidem*.

⁵¹ *Ibidem*.

Según los autores, establecer el derecho a monetizar permitiría que los usuarios finales reciban una compensación proporcional a su aporte informacional, lo que conduciría a un ecosistema digital más equitativo, inclusivo y sostenible⁵². Adicionalmente, algunos académicos argumentan que los usuarios deben recibir compensación no solo por proveer datos, sino también por los riesgos que esta cesión implica para su bienestar económico. Esto se debe a que las grandes empresas están recopilando información sin ofrecer retribución alguna, y luego utilizan esos datos para desarrollar inteligencia artificial que, eventualmente, reemplaza a los mismos usuarios en el mercado laboral. Esta dinámica genera un perjuicio financiero, lo que refuerza la necesidad de que la sociedad reciba un beneficio tangible por la información que entrega⁵³.

En esa línea, la Ley de Privacidad del Consumidor de California (CCPA)⁵⁴ representa un avance normativo significativo, al reconocer el valor monetario de los datos personales. Esta ley otorga a los consumidores un mayor control sobre la forma en que se recolecta y utiliza su información, y crea un mecanismo para que puedan monetizar sus datos. Si bien actualmente no ofrece una estructura concreta para que los consumidores obtengan ganancias económicas directas, representa un paso hacia la disrupción de los modelos tradicionales de intercambio de datos y la consolidación del derecho a monetizar la información personal. En el futuro cercano, es probable que otros gobiernos adopten esquemas similares para otorgar más privacidad, control y derechos de monetización a los ciudadanos.

Actualmente, la tecnología ya permite a los usuarios conocer el valor monetario de sus datos personales y monetizarlos efectivamente⁵⁵. Este valor puede estimarse tanto para los datos utilizados internamente por una empresa, como para aquellos vendidos a anunciantes o terceros.

⁵² *Ibidem*.

⁵³ *Ibidem*.

⁵⁴ California Consumer Privacy Act, Cal. Civ. Code §§ 1798.100-1798.199.

⁵⁵ Por ejemplo, revisar: Killi App <https://www.reclaimyours.com/>; Oceanprotocol <https://oceanprotocol.com/>; Swash <https://swashapp.io/>; Brave Browser <https://brave.com/>; Ernie App <https://ernieapp.com/>; Datum App <https://datum.org/>; Meeco <https://www.meeco.me/>; Mine App <https://www.saymine.com/>; De Datavakbond <https://datavakbond.nl/>; Datacoup <https://datacoup.com>. Consulta: 15 de abril de 2025.

La información puede mostrarse al usuario diferenciada por proveedor de servicios, de modo que en cada cuenta se visualice el valor generado. Parámetros como la frecuencia de uso y la tasa de conversión influyen directamente en la valorización del dato, al igual que las configuraciones de privacidad: a menor restricción, mayor potencial económico del dato⁵⁶.

Con el auge de la tecnología y las comunicaciones, este modelo de negocio ha demostrado ser altamente lucrativo. Empresas del rubro tecnología han generado ingresos sustanciales mediante el uso y análisis de los datos personales de los usuarios⁵⁷. Sin embargo, los individuos cuyos datos son utilizados para generar dicho valor rara vez reciben compensación directa. Esto plantea cuestiones fundamentales sobre la equidad, la justicia fiscal y la distribución del valor económico generado en la economía digital.

El DMDP, entonces, propone un cambio en la dinámica actual, bajo la cual únicamente las empresas del rubro tecnología generan ingresos sustanciales mediante el uso y análisis de los datos personales de los usuarios⁵⁸, siendo que los individuos –en adelante– tendrían el derecho legal a recibir una compensación monetaria por el uso de sus datos personales por parte de entidades comerciales⁵⁹. Esto implicaría el reconocimiento de los datos personales como un activo económico sobre el cual el titular tiene ciertos derechos patrimoniales.

La implementación del DMDP podría adoptar diversas formas. Una posibilidad sería un sistema en el que los usuarios puedan negociar directamente con las empresas el uso de sus datos. Alternativamente, podrían establecerse mecanismos regulatorios que obliguen a las empresas a compensar a los usuarios por la recopilación y uso de sus datos, por ejemplo, a través de pagos directos, sistemas de licencias o regalías.

⁵⁶ DE MICHELIS & BOLIGNINI, op. cit.

⁵⁷ Deloitte. (2019). Digital transformation through data: A guide for news and media companies to drive value with data. Google News Initiative. Recuperado de: <https://newsinitiative.withgoogle.com/articles/deloitte-digital-transformation-through-data/>

⁵⁸ *Ibid.*

⁵⁹ MOORE, S. (2015). How to monetize your customer data. Gartner; FRED, op. cit.

Este concepto no solo aborda la cuestión de la justicia económica, sino que también tiene importantes implicaciones fiscales. Si los usuarios comienzan a recibir ingresos por permitir el uso de sus datos, estos ingresos estarían sujetos a tributación. Esto, a su vez, plantea la necesidad de desarrollar marcos normativos claros sobre cómo deben tratarse dichos ingresos dentro del sistema fiscal de cada país.

A medida que más jurisdicciones enfrentan el reto de gravar la economía digital, el DMDP puede ofrecer una solución innovadora para asignar derechos fiscales a las jurisdicciones donde residen los usuarios y se generan los datos altamente apreciados. Esto permitiría a los países gravar de manera más equitativa los beneficios económicos generados por las empresas digitales, especialmente aquellas que operan sin presencia física en sus territorios.

Partiendo de la premisa donde los usuarios recibirán compensación económica bajo el esquema del DMDP, en la siguiente sección se abordarán los desafíos fiscales específicos que plantea la tributación de dichos ingresos.

V. Una propuesta de cambio: Monetización de la información y DMDP

En este apartado analizaremos los retos fiscales que enfrentan los individuos cuando empiezan a recibir ingresos derivados de la monetización de sus datos personales bajo un esquema de DMDP. La atención se centra tanto en problemas de diseño tributario como en aspectos administrativos y prácticos que podrían afectar la implementación eficaz del sistema.

El reconocimiento del DMDP como un derecho patrimonial de los usuarios en la economía digital representa un punto de inflexión en el diseño del sistema fiscal contemporáneo⁶⁰. Si los datos personales pasan a ser considerados activos generadores de valor económico (y, por lo tanto, susceptibles de generar renta imponible), ello implica necesariamente la revisión y adecuación del marco normativo que regula tanto la determinación de la renta como la obligación tributaria de los

⁶⁰ BURNS, L., & KREVER, R. (1998). Taxation of income from business and investment. En V. Thuronyi (Ed.), *Tax law design and drafting* (Vol. 2, pp. 1-69). International Monetary Fund.

contribuyentes y/o responsables. Sin embargo, esta transición no está exenta de retos técnicos, jurídicos y administrativos.

i. Calificación jurídica de los ingresos percibidos por DMDP

Uno de los principales retos es la calificación tributaria del ingreso percibido por los usuarios como contraprestación por el uso de sus datos personales. En términos doctrinales, la dificultad radica en determinar si dicho ingreso se encuadra como:

- Ganancia de capital, en tanto producto de la cesión de un activo intangible auto-generado;
- Renta del trabajo independiente, si existe habitualidad y carácter empresarial;
- Ingreso esporádico o incidental, si se trata de microtransacciones no recurrentes.

Indudablemente, superar este primer nivel de discusión es fundamental; siendo que esta indeterminación genera inseguridad jurídica y sería obstáculo del cumplimiento tributario efectivo⁶¹. A nivel práctico, ello incide directamente en aspectos como la identificación del tipo de impuesto aplicable (renta, dividendos, regalías), la aplicabilidad de retenciones, y la deducción de gastos (difícilmente atribuibles, puesto que los datos no tienen costo de adquisición claro).

De cualquier modo, la imposición directa sobre los usuarios por los ingresos derivados del DMDP presenta dificultades prácticas y estructurales. Así pues, bajo el sistema propuesto, en lugar de gravar directamente a los usuarios, el impuesto recaería sobre las empresas multinacionales (MNEs), y se calcularía a una tasa fija sobre el monto total pagado a los usuarios en una jurisdicción determinada.

Esta propuesta se inspira en un sistema de Impuesto sobre Distribución de Dividendos (“DDT”), en virtud del cual los dividendos estarían exentos para los accionistas, pero la empresa distribuidora debía abonar el impuesto correspondiente sobre las utilidades distribuidas; lo que

⁶¹ MILOT, L. (2010). What are we – Laborers, factories, or spare parts? The tax treatment of transfers of human body materials. *Washington and Lee Law Review*, 67(3), pp. 1053-1132; BURNS & KREVER, op. cit.

sucedía, por ejemplo, en la India⁶². Dicho ingreso estaría exonerado de imposición en manos del usuario final⁶³.

ii. Problemas de valoración objetiva de los datos

Una dificultad adicional y sustancial es la valoración económica del ingreso derivado del DMDP, especialmente cuando los datos no son transferidos a terceros mediante un precio de mercado, sino usados internamente para fines algorítmicos (como perfiles, inteligencia artificial o publicidad dirigida). En estos casos, no existe un valor observable de transacción, lo que plantea retos para la determinación de la base imponible⁶⁴.

Si bien existen aproximaciones indirectas –como el valor promedio de los datos en plataformas publicitarias– no hay consenso metodológico global. La OCDE, en informes como *Taxing the Digital Economy* (2020), ha reconocido la falta de transparencia en las estructuras de precios de los activos informacionales, lo cual dificulta su tributación justa y eficaz.

iii. Atomización de contribuyentes y eficiencia administrativa

Una de las características propias del modelo DMDP es que la base de usuarios es amplia, dispersa y con ingresos individualmente reducidos. Esto significa que millones de contribuyentes podrían percibir montos bajos (a menudo por debajo del umbral mínimo no imponible). La implicancia práctica es clara: el costo administrativo de fiscalizar individualmente a esta masa de contribuyentes superaría, con alta probabilidad, la recaudación potencial⁶⁵.

⁶² Véase Sección 115-O of the Indian Income-tax Act, 1961

⁶³ Véase *Godrej & Boyce Manufacturing Company Ltd. v. DCIT* (2017) (81 taxmann. com 111) (Corte Suprema), en el cual la Corte Suprema de la India sostuvo que el Impuesto sobre Distribución de Dividendos (DDT) debe considerarse como un impuesto aplicado sobre las utilidades distribuidas de la empresa.

⁶⁴ FEYGIN, Y., HECHT, B. et al. (2021). *A data dividend that works: Steps toward building an equitable data economy*. Berggruen Institute.

⁶⁵ OECD Forum on Tax Administration. (2022, 28 de septiembre). *Tax Administration 3.0 and the Digital Identification of Taxpayers: Initial Findings*. OECD Publishing. <https://doi.org/10.1787/3ab1789a-en>.

En consecuencia, se hace necesaria la implementación de mecanismos de cumplimiento simplificado⁶⁶, tales como:

- Regímenes de retención en la fuente por parte de las plataformas digitales;
- Sistemas automáticos de reporte y declaración;
- Umbrales de exoneración, con tributos aplicables solo a montos acumulados relevantes.

iv. Doble imposición internacional y nexo fiscal digital

La dimensión transfronteriza del ecosistema digital amplifica los desafíos fiscales del DMDP. Dado que los usuarios pueden residir en una jurisdicción diferente de aquella donde se encuentra la empresa que monetiza sus datos, se genera un riesgo claro de doble imposición internacional, así como de vacíos de imposición.

Por ejemplo, una plataforma radicada en Irlanda podría monetizar datos de usuarios ubicados en Perú, India o México. Si el ingreso no es gravado en origen ni reconocido en destino, se produce una erosión de la base imponible. Si, por el contrario, ambas jurisdicciones pretenden gravarlo, el resultado sería la doble imposición. Este problema se agrava por la ausencia de un nexo físico, lo que debilita las potestades tradicionales de imposición territorial.

El principio de asignación de derechos fiscales a la jurisdicción de mercado, que subyace en el Pilar Uno del proyecto BEPS de la OCDE, se alinea con la lógica del RTM y podría servir como base normativa para resolver esta tensión.

v. Obligaciones formales y capacidad de cumplimiento

Finalmente, existen dudas significativas respecto a las obligaciones formales de los usuarios individuales bajo un esquema de monetización de datos. La mayoría carece de capacidad técnica o financiera para registrar ingresos mínimos, determinar su naturaleza fiscal, aplicar retenciones o emitir comprobantes tributarios. Del lado de las plataformas, tampoco existe hoy una infraestructura obligatoria y uniforme que les exija actuar como agentes de retención o como emisores de reportes automatizados.

⁶⁶ *Ibid.*

En este sentido, una propuesta que planteamos es la creación de un sistema de Identificación Tributaria Digital Única⁶⁷ (ITDU) y el uso de tecnologías distribuidas (blockchain) para automatizar el cumplimiento sin exigir intervención directa de los usuarios. Justamente, el código de ITDU consistiría en un cifrado alfanumérico de formato universal, cuyos caracteres incluirían información que permita identificar el país de residencia del usuario. Por ejemplo, a cada usuario se le asignaría una única ITDU, y si este cambiase de país de residencia (o de acceso), los caracteres correspondientes al país dentro del código se actualizarían automáticamente, en función de la dirección IP.

Asimismo, las MNEs que recolectan datos de los usuarios también estarían obligadas a obtener un ITDU. Este sistema tendría interoperabilidad transfronteriza, y los usuarios que deseen monetizar sus datos estarían obligados a proporcionar su ITDU a la MNE que efectúe el pago correspondiente ante la autoridad tributaria respectiva.

VI. Reflexiones finales

Como se ha expuesto, el Pilar Uno representa la propuesta de la OCDE destinada a transformar el sistema tributario internacional para hacer frente a los desafíos surgidos de la digitalización de la economía. A través del Monto A y las pautas relacionadas con el nexo, además del origen de los ingresos, el objetivo del aludido Pilar es abordar completa y definitivamente dichos desafíos. No obstante, persisten diversos problemas que requieren de soluciones o, cuando menos, propuestas de remedios.

⁶⁷ Este sistema propuesto de UDTIN sigue una lógica similar a la del código de Identificador de Entidad Legal (“LEI”, por sus siglas en inglés) para transacciones financieras, o al Número Internacional de Cuenta Bancaria (“IBAN”) utilizado por las instituciones bancarias. El código LEI es un identificador alfanumérico de 20 caracteres que se asigna a las personas jurídicas y actúa como un directorio global para identificar entidades legales a nivel mundial. Global Legal Entity Identifier Foundation (GLEIF). Introducing the Legal Entity Identifier (LEI): About LEI. GLEIF. Recuperado el 15 de febrero de 2025, de <https://www.gleif.org>. Por su parte, el IBAN es un sistema de numeración internacionalmente aceptado que permite identificar de manera única la cuenta bancaria de un cliente. El IBAN está compuesto por un código de país alfabético, seguido por dos dígitos de control, y posteriormente hasta treinta y cinco caracteres que representan el número de cuenta bancaria. (IBAN. (s. f.). List of abbreviations used in bank funds transfers. IBAN. Recuperado el 15 de febrero de 2025, de <https://www.iban.com/glossary>).

Aunque las opiniones podrían revelarse en el mismo sentido y aceptar la necesidad de una solución global para gravar la economía digital, todavía es cierto que esto demanda que la implementación práctica sea viable para todos los operadores involucrados. Además, es vital que se cumpla con los principios de neutralidad, certeza y simplicidad para la creación de tal imposición.

Bajo esta lógica, conviene recordar que la complejidad asociada a la introducción de una nueva norma podría tornarla impracticable y generar costos administrativos elevados, tanto para las autoridades fiscales como para las grandes empresas (quienes, en principio, serían el “target” de estas herramientas)⁶⁸. En el caso peruano, la experiencia de este tipo de obstáculos predomina.

Por su lado, entendiendo que las disposiciones del Pilar Uno pueden ser sujetas de evaluación, sería conveniente preguntarnos si modificar las reglas actuales de nexo y origen de los ingresos servirá como soporte de su implementación. De esta manera, con la dificultad que implica tratar de reflejar y adaptarse a la diversidad de lo existente en diferentes geografías, las reglas del Pilar Uno podrían sumar partidarios y volverse más flexibles, siempre sobre la premisa de ser una herramienta enfocada al incremento de la simplicidad de las empresas.

De cualquier modo, su implementación paralela junto con las reglas fiscales internacionales actualmente vigentes amplía la idea de que el Pilar Uno sea solamente una medida provisional, y que quizás no se perciba como la solución definitiva ni a largo plazo. Más aún, debido a la preexistencia de criterios, llegará el momento de responder de manera objetiva a la pregunta de si la implementación del mencionado Pilar beneficiará a la mayoría de las jurisdicciones o si sus ventajas solo serán aprovechadas por algunos⁶⁹.

Por otro lado, el surgimiento de la economía digital y la expansión de los modelos de negocio basados en datos han generado desafíos inéditos en el ámbito de la fiscalidad internacional. Las MNEs están utilizando los datos personales de los usuarios para generar beneficios significativos, lo

⁶⁸ SALAS, L. (2023). Nexus and revenue sourcing rules under OECD Pillar One. En M. Lang (Ed.), *Series on International Tax Law* (Vol. 137, pp. 123). IBFD.

⁶⁹ VAN DAM, VÁZQUEZ, BURIAL & KUNEN, op. cit.

cual resalta la relevancia del concepto emergente de derecho a monetizar los datos (DMDP). Este artículo explora dicho concepto, en virtud del cual los usuarios individuales podrían recibir una compensación monetaria por parte de las MNEs por la utilización económica de sus datos personales.

En particular, la tesis plantea la creación de un Número Único de Identificación Tributaria Digital (ITDU) y un sistema de reporte basado en accesos digitales. El ITDU permitiría a las MNEs agrupar y consolidar los pagos realizados a usuarios por jurisdicción, y calcular así la obligación tributaria total correspondiente en cada país. Integrado a las plataformas digitales, el ITDU facilitaría la transparencia fiscal y reduciría los riesgos de evasión.

Finalmente, el traslado de la carga tributaria del usuario a las MNEs respecto de los ingresos generados por el RTM, combinado con un enfoque centrado en el usuario y apoyado en infraestructuras digitales como el UDTIN, constituye una solución prometedora para reconocer los derechos fiscales de las jurisdicciones de mercado. Con investigación continua, voluntad política y cooperación internacional, es posible construir un sistema fiscal más justo y eficaz para la era digital.

Algoritmos opacos y privacidad diferencial: ¿puede haber transparencia sin comprometer la protección?

Juan Emmanuel Delva Benavides*
y Vania Valeria Mendez Gonzalez**

Resumen.- El presente artículo analiza la tensión entre transparencia algorítmica y privacidad diferencial en el contexto de implementación creciente de sistemas de Inteligencia Artificial en ámbitos sensibles. A través de un análisis interdisciplinario que integra perspectivas jurídicas, tecnológicas y éticas, se examina cómo los algoritmos opacos comprometen la rendición de cuentas y cómo la privacidad diferencial, aunque protege datos personales, puede socavar la exactitud algorítmica.

Palabras clave.- Algoritmos opacos – privacidad diferencial – transparencia algorítmica – protección de datos – inteligencia artificial – derecho digital.

Abstract.- This article analyzes the tension between algorithmic transparency and differential privacy in the context of increasing implementation of Artificial Intelligence systems in sensitive areas. Through an interdisciplinary analysis that integrates legal, technological, and ethical perspectives, it examines how opaque algorithms compromise accountability and how differential privacy, while protecting personal data, can undermine algorithmic accuracy.

Keywords.- Opaque algorithms – Differential privacy – Algorithmic transparency – Data protection – Artificial intelligence – Digital law.

* Profesor Investigador en la Universidad de Guadalajara. Doctor en Derecho, maestro en tecnologías y abogado por parte de la UdeG. Socio fundador de la Asociación Latinoamericana de Derecho, Gobierno y Nuevas Tecnologías.

** Estudiante de la carrera de Negocios Internacionales de la Universidad de Guadalajara y técnico en programación por parte del Centro de Bachilleres Industriales y Tecnológicos.

I. Introducción

Desde inicios del siglo XXI, la humanidad está experimentando una transformación digital sin precedentes, comparable quizás solo con la revolución industrial del siglo XVIII. La diferencia fundamental radica en que, mientras la revolución industrial transformó nuestra relación con el mundo físico, la revolución digital está reconfigurando nuestra existencia informacional y cognoscitiva. A modo de ilustración, si la máquina de vapor permitió multiplicar la fuerza física humana, los algoritmos de inteligencia artificial están amplificando –y en algunos casos, sustituyendo– nuestras capacidades cognitivas y decisorias.

La sociedad contemporánea se caracteriza por una hiperconectividad creciente¹, donde el trabajo, la educación, el comercio e incluso las interacciones sociales están mediados por tecnologías digitales. Esta transformación se refleja en cifras contundentes: 4.88 billones de usuarios de Internet a nivel global en 2021, con un 62% de la población mundial utilizando redes sociales². En México, el panorama no es diferente: el INEGI (2024) reporta que el 68.5% de los hogares mexicanos –equivalente a 25.8 millones– cuenta con acceso a Internet³.

Esta digitalización masiva ha catalizado el surgimiento de lo que podríamos denominar la “economía del dato”, un ecosistema donde la información personal se ha convertido en el petróleo del siglo XXI. En este contexto, los corredores de datos o *data brokers* operan como nuevos intermediarios, recolectando y comercializando información de diversas fuentes para su posterior análisis. Al igual que ocurrió con los recursos naturales en siglos anteriores, estamos presenciando una “carrera por el dato” donde empresas y gobiernos compiten por capturar, procesar y monetizar la mayor cantidad posible de información personal.

-
- ¹ DURAO, M.; ETCHEZAHAR, E.; GÓMEZ, T.; MULLER, M. (2024). *Hiperconectados: Los desafíos psicológicos de la era digital*. Madrid, España: TechPsyLab
- ² DataReportal. (2021). Digital 2021 october global statshot report. <https://datareportal.com/reports/digital-2021-october-global-statshot>
- ³ INEGI (Instituto Nacional de Estadística y Geografía). (2024). Estadísticas a propósito del Día Mundial del Internet. https://inegi.org.mx/contenidos/salade_prensa/aproposito/2024/EAP_DMInternet.pdf

El aprovechamiento comercial de estos datos ocurre a través de múltiples vías: desde políticas de privacidad que autorizan la cesión a terceros, hasta tecnologías como las *cookies* que monitorizan en tiempo real los patrones de comportamiento digital. Como en el caso del legendario caballo de Troya, detrás de la aparente gratuidad de muchos servicios digitales se esconde un mecanismo sofisticado de captura de datos personales.

Las empresas suelen justificar estas prácticas argumentando que los datos son “anonimizados”, eliminando identificadores directos. Sin embargo, como demuestra Narayanan⁴, existen numerosos “vectores de fuga” que posibilitan la reidentificación de individuos mediante la correlación de diferentes conjuntos de datos aparentemente anónimos. Es comparable a un rompecabezas donde, aunque faltan piezas individuales, la imagen completa puede reconstruirse mediante la combinación inteligente de fragmentos dispersos.

Es en este contexto donde emergen y adquieren relevancia crítica los conceptos de algoritmos opacos y privacidad diferencial, representando dos valores aparentemente contrapuestos: por un lado, la necesidad de transparencia en los sistemas algorítmicos que toman decisiones con impacto significativo en la vida de las personas; por otro, la imprescindible protección de la privacidad en un entorno de dataficación masiva.

El presente artículo examina esta tensión fundamental y busca responder a una pregunta central para el Estado de Derecho en la era digital: ¿Es posible construir sistemas algorítmicos que sean simultáneamente transparentes –y, por tanto, auditables– y respetuosos de la privacidad? ¿O estamos ante un dilema irresoluble donde debemos sacrificar un valor en aras del otro?

La tensión entre algoritmos opacos y privacidad diferencial representa, más que un dilema técnico pasajero, una manifestación concreta del conflicto fundamental que toda sociedad democrática debe resolver en la era digital: cómo equilibrar transparencia, privacidad, seguridad y eficiencia. Esta disyuntiva evoca la clásica tensión entre libertad

⁴ NARAYANAN, A. (2011). There is no such thing as anonymous online tracking. The Center for Internet and Society at Stanford Law School. <http://cyberlaw.stanford.edu/blog/2011/07/there-no-such-thing-anonymous-online-tracking>. (Fecha de consulta: 02 de mayo de 2025).

y seguridad que ha definido los debates constitucionales desde la Ilustración, pero con un elemento distintivo y perturbador: la velocidad vertiginosa con que la tecnología reconfigura los términos del debate, comparable quizás a cómo la imprenta de Gutenberg transformó las estructuras de poder informacional en el siglo XV, pero a una escala exponencialmente acelerada. Mientras que la sociedad tardó décadas en adaptar sus estructuras regulatorias a la imprenta, hoy enfrentamos cambios paradigmáticos en ciclos de meses o incluso semanas.

Dicho esto, este trabajo parte de la hipótesis de que a pesar de la tensión entre la privacidad de los usuarios y la necesidad de la transparencia en el tratamiento de dichos datos -para que sean auditables-, es posible diseñar mecanismos que permitan mantener ambas variables sin que una comprometa a la otra.

II. Marco Teórico Conceptual: Entre la Opacidad y la Distorsión

i. Algoritmos opacos: Las cajas negras decisorias

Los algoritmos opacos representan una de las paradojas más significativas de la era digital: sistemas cada vez más determinantes en nuestras vidas, pero simultáneamente inescrutables en su funcionamiento interno. El término “caja negra”, prestado de la ingeniería de sistemas, ilustra perfectamente esta contradicción: podemos observar lo que entra (datos) y lo que sale (decisiones), pero el proceso intermedio permanece oculto, incluso para sus propios creadores.

Esta opacidad no es meramente técnica, sino inherente a la naturaleza de los sistemas de aprendizaje automático contemporáneos (*Machine Learning*). A diferencia de la programación tradicional, donde un desarrollador codifica explícitamente cada regla lógica, el aprendizaje automático genera sus propios modelos a partir del análisis de enormes cantidades de datos, creando redes neuronales complejas cuyo funcionamiento interno resulta prácticamente indescifrable⁵.

Para dimensionar adecuadamente el problema, imaginemos un juez humano que tomara decisiones sin explicar jamás su razonamiento, o un médico que diagnosticara enfermedades sin revelar qué síntomas

⁵ HURSHMAN, C. “¿Tienen funciones los algoritmos opacos?” En *Synthese*, 204, 91 (2024). <https://doi.org/10.1007/s11229-024-04745-2>

o pruebas considera relevantes. Tal escenario resultaría inaceptable en contextos profesionales humanos, pero es precisamente lo que ocurre con muchos sistemas algorítmicos que ya están operando en ámbitos críticos como la justicia penal, la medicina diagnóstica o la evaluación crediticia.

ii. Privacidad diferencial: El arte de ocultar mostrando

Como contrapunto a la transparencia algorítmica, la privacidad diferencial emerge como un enfoque matemático que busca proteger la información personal mientras permite el análisis agregado de datos. Desarrollada inicialmente por Dwork⁶, esta metodología utiliza la distorsión controlada —añadiendo “ruido” estadístico calibrado— para garantizar que la presencia o ausencia de un individuo en una base de datos no afecte significativamente los resultados del análisis.

La privacidad diferencial podría compararse con una técnica fotográfica que deliberadamente desenfoca ciertos elementos de la imagen para proteger identidades específicas, manteniendo a la vez la nitidez suficiente para interpretar la escena general. El desafío radica en determinar el nivel óptimo de “desenfoque” que proteja adecuadamente sin comprometer excesivamente la utilidad analítica de los datos.

iii. La dialéctica entre transparencia y privacidad

La tensión entre transparencia algorítmica y privacidad diferencial puede conceptualizarse como una relación inversamente proporcional: cuanto mayor es la transparencia, mayor el riesgo para la privacidad; y cuanto más robusta la protección de privacidad, menos precisos o transparentes resultan los algoritmos.

Esta relación inversamente proporcional evoca el principio de incertidumbre de Heisenberg en física cuántica⁷; así como es imposible

⁶ DWORK, C. (2006). Differential Privacy. 33rd International Colloquium on Automata, Languages and Programming, pp. 1-12.

⁷ HEISENBERG, W. (1927). Über den anschaulichen Inhalt der quantentheoretischen Kinematik und Mechanik. Zeitschrift für Physik, 43(3-4), pp. 172-198. Esta referencia alude al principio físico que establece la imposibilidad de determinar simultáneamente con precisión absoluta la posición y el momento de una partícula. La analogía aplicada al contexto de algoritmos sugiere que existe una limitación

conocer simultáneamente y con precisión absoluta la posición y el movimiento de una partícula, parece existir una limitación fundamental para lograr simultáneamente máxima transparencia algorítmica y máxima protección de la privacidad.

III. Tensión entre Transparencia y Privacidad: Un Análisis Multidimensional

i. El imperativo ético de la transparencia

La transparencia algorítmica constituye un requisito fundamental para la rendición de cuentas en sociedades democráticas. Cuando los algoritmos determinan quién obtiene un préstamo, quién recibe tratamiento médico prioritario o quién representa un riesgo para la seguridad pública, su funcionamiento no puede permanecer como una “caja negra” impenetrable.

El caso emblemático de COMPAS (Correctional Offender Management Profiling for Alternative Sanctions) en Estados Unidos ilustra claramente esta problemática. Este sistema, utilizado para evaluar el riesgo de reincidencia criminal, ha sido objeto de intenso escrutinio tras el análisis de ProPublica⁸ que reveló sesgos raciales significativos. Sin embargo, la empresa desarrolladora se ha negado a revelar completamente el funcionamiento interno del algoritmo, argumentando protección de propiedad intelectual y secretos comerciales.

Este caso evidencia cómo la opacidad algorítmica puede socavar principios fundamentales del debido proceso: ¿cómo puede un acusado defenderse efectivamente si desconoce la lógica que lo clasifica como “alto riesgo”? Es comparable a un juicio donde la prueba determinante permanece sellada, inaccesible tanto para el acusado como para su defensa.

fundamental entre la transparencia completa de un sistema algorítmico y la protección total de la privacidad de los datos que utiliza.

⁸ ANGWIN, J; LARSON, J; MATTU, S. & KIRCHNER, L. (2024). Machine Bias: There's software used across the country to predict future criminals. And it's biased against blacks. ProPublica.

ii. El imperativo legal de la privacidad

Por otra parte, la protección de datos personales constituye un derecho fundamental reconocido en marcos normativos como el Reglamento General de Protección de Datos (GDPR) europeo o la Ley Federal de Protección de Datos Personales en Posesión de Particulares en México. Estos marcos exigen que los datos personales sean tratados con medidas técnicas y organizativas que garanticen su confidencialidad e integridad.

La privacidad diferencial ofrece una solución técnica prometedora para este imperativo legal. Sin embargo, como demuestra Salaberry⁹, esta metodología implica un compromiso inevitable entre privacidad y precisión: cuanto más se protege la privacidad mediante la adición de “ruido” estadístico, menos precisos resultan los datos para análisis posteriores.

iii. La paradoja de la explicabilidad computacional

La tensión entre transparencia y privacidad se manifiesta técnicamente en lo que podríamos denominar “la paradoja de la explicabilidad”. Los investigadores Tramer¹⁰ y Shokri et al.¹¹ han demostrado que los modelos completamente transparentes son vulnerables a lo que se conoce como “ataques de inversión” o “ataques de membresía”, mediante los cuales un adversario puede inferir si determinados datos individuales formaron parte del conjunto de entrenamiento del modelo.

Este fenómeno es comparable a cómo un estudiante podría deducir el contenido exacto de un examen futuro si tuviera acceso completo al proceso mental del profesor que lo diseña. La transparencia total, paradójicamente, puede comprometer la integridad del sistema que se pretende explicar.

⁹ SALABERRY, N. (2020). Gestión de la privacidad de datos personales: el modelo de privacidad diferencial. *Revista de Investigación En Modelos Matemáticos Aplicados A la Gestión y la Economía*, II (2020-II), pp. 45-67.

¹⁰ TRAMER, F. (2023). Modelo de inversión de ataques: Desafíos para la privacidad en la era de modelos transparentes. *IEEE Symposium on Security and Privacy*, 432-449.

¹¹ SHOKRI, R; STRONATI, M; SONG, C. & SHMATIKOV, V. (2021). Membership Inference Attacks Against Machine Learning Models. *IEEE Symposium on Security and Privacy*, pp. 3-18.

IV. Casos de estudio sectoriales

La tensión entre transparencia algorítmica y privacidad diferencial se manifiesta de manera particular en sectores críticos donde los algoritmos están transformando radicalmente los procesos decisorios. Al igual que la invención de la imprenta revolucionó el acceso al conocimiento en el siglo XV, los algoritmos de aprendizaje profundo están reconfigurando industrias enteras, pero con una diferencia fundamental: mientras que los libros impresos exponían abiertamente su contenido, los algoritmos contemporáneos ocultan sus mecanismos internos tras capas de complejidad matemática.

En el sector sanitario, asistimos a una revolución diagnóstica comparable a la introducción del microscopio en el siglo XVII. Los algoritmos de diagnóstico médico basados en redes neuronales convolucionales, como los desarrollados por Google Health para la detección de retinopatía diabética, han demostrado una precisión diagnóstica que iguala o supera a oftalmólogos experimentados¹². Sin embargo, a diferencia del médico que puede explicar paso a paso su razonamiento clínico, estos sistemas funcionan como “oráculos digitales” que emiten veredictos sin revelar su lógica interna. Esta opacidad plantea dilemas éticos fundamentales: ¿cómo puede un paciente otorgar consentimiento verdaderamente informado cuando ni siquiera los desarrolladores del algoritmo comprenden completamente por qué el sistema llega a determinada conclusión? Simultáneamente, la extrema sensibilidad de los datos médicos —que pueden revelar desde predisposiciones genéticas hasta comportamientos íntimos— exige mecanismos robustos de privacidad diferencial, creando una tensión aparentemente irresoluble entre explicabilidad y confidencialidad.

El sector financiero ofrece otro escenario paradigmático donde esta tensión adquiere dimensiones socioeconómicas significativas. Los sistemas algorítmicos de evaluación crediticia, como el FICO Score en Estados Unidos o el Buró de Crédito en México, han evolucionado desde

¹² GULSHAN, V; PENG, L; CORAM, M; STUMPE, M. C.; WU, D & NARAYANASWAMY, A. (2016). Development and validation of a deep learning algorithm for detection of diabetic retinopathy in retinal fundus photographs. *Journal of the American Medical Association*, 316 (22), pp. 2402-2410.

simples modelos estadísticos hasta complejos sistemas de aprendizaje automático que analizan cientos de variables para determinar la solvencia de un solicitante. Como señalan Martínez-Plumed et al. (2024), estos algoritmos frecuentemente “perpetúan y amplifican desigualdades históricas al incorporar variables proxy que correlacionan con características protegidas como raza o género”¹³.

La forma en que los sistemas de evaluación crediticia funcionan y han evolucionado a lo largo del tiempo es compleja. Desde que se fundó la primera agencia de informes crediticios en EE. UU. Se comenzó utilizando métodos en donde se evaluaban los informes, se clasificaba el riesgo crediticio y se modelaba la información estadísticamente en modelos lineales en el que usaban información como socioeconómica general, demográfica y de ingresos variables, utilizando las suposiciones en el que el comportamiento pasado del consumidor es un indicador del comportamiento futuro¹⁴. Mientras que, en los actuales métodos de evaluación crediticia utilizando aprendizaje automatizado se utilizan modelos basados en árboles en donde se utilizan cientos de variables en tiempo real para predecir la capacidad de pago de una persona, posibilitando, por un lado, una predicción más precisa, pero al mismo tiempo deja un posible sesgo algorítmico donde se trata de evocar la explicabilidad y transparencia de los datos obtenidos.

Esta situación evoca la parábola kafkiana del guardián de la ley: ciudadanos que permanecen eternamente a las puertas del sistema financiero, sin comprender las reglas invisibles que determinan su exclusión. Paradójicamente, las técnicas de privacidad diferencial, al “difuminar” los datos individuales, pueden simultáneamente proteger la privacidad de los consumidores mientras oscurecen aún más los

¹³ ADEYELU, O. O; UGOCHUKWU, C. E. & SHONIBARE, M. A. (2024). Ethical implications of AI in financial decision-making: A review with real-world applications. *International Journal of Applied Research in Social Sciences*, 6 (4), pp. 608-630.

¹⁴ MALEMPATI, M. (2025). The evolution of credit data and the role of machine learning in modern credit scoring. In *The Intelligent Ledger: Harnessing Artificial Intelligence, Big Data, and Cloud Power to Revolutionize Finance, Credit, and Security* (pp. 19-35). Deep Science Publishing. https://doi.org/10.70593/978-93-49910-16-4_2

patrones discriminatorios subyacentes, creando una “opacidad de segundo orden” que dificulta la auditoría de sesgos algorítmicos¹⁵.

Quizás el caso más emblemático de esta tensión se manifiesta en el sector judicial, donde algoritmos como COMPAS están siendo implementados para tareas tan sensibles como la evaluación de riesgos procesales o la recomendación de sentencias. La investigación de ProPublica reveló que este sistema “clasificaba incorrectamente a acusados afroamericanos como “alto riesgo” casi el doble de veces que, a acusados caucásicos, evidenciando sesgos sistémicos”¹⁶. Sin embargo, la empresa desarrolladora, Northpointe (ahora Equivant), se negó a revelar completamente el funcionamiento interno del algoritmo, argumentando protección de propiedad intelectual. Este caso ilustra vívidamente la colisión entre el derecho empresarial a proteger secretos comerciales y principios fundamentales del debido proceso como el derecho a confrontar la evidencia adversa. Es comparable a un sistema judicial medieval donde las pruebas determinantes permanecían selladas en cofres inaccesibles para el acusado, con la particularidad de que, en la era digital, estos “cofres algorítmicos” están protegidos no solo por cerraduras físicas sino por capas de complejidad matemática y protecciones legales de propiedad intelectual.

IV. Soluciones Intermedias: Hacia una Conciliación Pragmática

Ante esta aparente contradicción entre valores igualmente importantes, diversas aproximaciones técnicas, legales y procedimentales ofrecen vías intermedias prometedoras. En primer lugar se encuentra la “Explicabilidad por capas”. La aparente contradicción entre la necesaria transparencia de sistemas algorítmicos que toman decisiones críticas y la imprescindible protección de datos personales no constituye necesariamente un dilema irresoluble. Al igual que en la arquitectura de seguridad nuclear se desarrollan “sistemas de defensa en profundidad” con múltiples capas de protección, el concepto de “explicabilidad

¹⁵ JOSHUA, A. Kroll; HUEY, Joanna; BAROCAS, Solon; FELTEN, Edward W; REIDENBERG, Joel R; ROBINSON, David G & HARLAN, Yu Accountable Algorithms, 165 U. Pa. L. Rev. 633 (2017).

¹⁶ ANGWIN, J; LARSON, J; MATTU, S & KIRCHNER, L. (2024). Machine Bias: There’s software used across the country to predict future criminals. And it’s biased against blacks. ProPublica.

por capas” propone un enfoque estratificado que modula el nivel de transparencia según el contexto, necesidad y audiencia legítima ¹⁷.

Este modelo puede estructurarse como un sistema concéntrico de acceso diferenciado a la información algorítmica. En el núcleo, encontraríamos una “capa técnica profunda” reservada para auditorías técnicas independientes y reguladores especializados, bajo condiciones estrictas de confidencialidad. Esta capa permitiría el escrutinio completo del código, parámetros y conjuntos de entrenamiento del algoritmo, similar al acceso que tienen los inspectores del Organismo Internacional de Energía Atómica (OIEA) a instalaciones nucleares sensibles: completo, pero estrictamente controlado mediante protocolos de seguridad multinivel.

Rodeando este núcleo, una “capa procesal intermedia” estaría dirigida específicamente a los sujetos directamente afectados por decisiones algorítmicas. Por ejemplo, un solicitante de crédito rechazado recibiría una explicación personalizada que identifica los factores específicos que determinaron su caso particular (como relación deuda-ingresos, historial de pagos atrasados o duración del historial crediticio), sin necesidad de comprender la compleja matemática del modelo subyacente. Esta aproximación se alinea con lo que Wachter *et al.* (2023)¹⁸ denominan “Explicaciones Contrafácticas”: respuestas a la pregunta “¿qué tendría que cambiar en mi situación para obtener un resultado diferente?”.

Finalmente, la capa más externa, o “capa conceptual superficial”, estaría orientada al público general, ofreciendo una comprensión accesible de los principios que rigen el sistema, sus objetivos declarados, limitaciones conocidas y mecanismos de supervisión. Esta capa funcionaría como un “prospecto algorítmico” comparable a los prospectos farmacéuticos que informan sobre medicamentos sin revelar la fórmula química exacta, permitiendo un escrutinio público significativo sin comprometer secretos comerciales ni facilitar la manipulación malintencionada del sistema.

¹⁷ CHEN, L; CRUZ, I; SHERIFF, S & KAMAR, E. (2024). Layered explanations: A practical framework for AI transparency. *Proceedings of the 2024 ACM Conference on Fairness, Accountability, and Transparency*, pp. 134-145.

¹⁸ WACHTER, S; MITTELSTADT, B & RUSSELL, C. (2023). Counterfactual Explanations without Opening the Black Box: Automated Decisions and the GDPR. *Harvard Journal of Law & Technology*, 36 (2), pp. 841-887.

Esta aproximación estratificada puede implementarse técnicamente mediante diversos métodos de “interpretabilidad *post-hoc*” como los mapas de saliencia en redes neuronales convolucionales o los modelos sustitutos interpretables (*surrogate models*), que generan aproximaciones simplificadas pero fieles de sistemas más complejos. La ventaja fundamental de este enfoque es que permite equilibrar la rendición de cuentas democrática con la protección de intereses legítimos de privacidad y propiedad intelectual, adaptando el nivel de explicabilidad al contexto específico y a la necesidad concreta de cada parte interesada.

Por otra parte, el desafío de proteger datos sensibles sin sacrificar la utilidad analítica o la transparencia algorítmica ha estimulado el desarrollo de técnicas avanzadas que podríamos denominar “privacidad por diseño”. Estas aproximaciones van más allá de la mera anonimización superficial, incorporando protecciones de privacidad en la arquitectura misma de los sistemas algorítmicos, comparable a cómo los principios de seguridad pasiva se incorporan estructuralmente en el diseño arquitectónico de edificios resistentes a sismos.

El “aprendizaje federado” representa una revolución paradigmática en este ámbito, comparable al paso de sistemas centralizados de agua potable a sistemas de captación pluvial distribuidos. En lugar de concentrar datos sensibles en servidores centrales vulnerables a brechas de seguridad, esta metodología desarrollada inicialmente por Google¹⁹ permite entrenar algoritmos de forma distribuida manteniendo los datos personales en los dispositivos de los usuarios y compartiendo únicamente modelos agregados. Un ejemplo concreto lo encontramos en la aplicación *SwiftKey*, que mejora sus predicciones de texto analizando patrones de escritura individuales sin jamás transmitir el contenido exacto de los mensajes a servidores centrales²⁰.

¹⁹ LI, T; SAHU; A. K., TALWALKAR, A & SMITH, V. (2024). Federated Learning: Challenges, Methods, and Future Directions. *IEEE Signal Processing Magazine*, 41 (3), pp. 148-170

²⁰ Microsoft. (s. f.). Microsoft SwiftKey Keyboard: Privacy Questions and your Data. Microsoft Support. Recuperado el 9 de mayo de 2025, de <https://support.microsoft.com/en-us/topic/microsoft-swiftkey-keyboard-privacy-questions-and-your-data-07e13677-6b38-4ad0-bad0-d41207cab6de>

Complementariamente, la técnica de “distilación de conocimiento”, conceptualizada originalmente por Geoffrey Hinton²¹, posibilita crear modelos simplificados que capturan la funcionalidad esencial de sistemas más complejos sin incorporar datos sensibles del modelo original. Esta aproximación es comparable a cómo un maestro transmite conocimiento esencial a un alumno sin revelar todas sus fuentes originales o experiencias personales.

Asimismo, la “computación multipartita segura” ofrece un enfoque prometedor para escenarios donde múltiples entidades necesitan computar conjuntamente funciones sobre sus datos privados sin revelarlos entre sí. Esta metodología, fundamentada en resultados teóricos de criptografía moderna, es comparable a una mesa de póker virtual donde cada jugador puede verificar que el juego es justo sin ver las cartas de los demás.

Estas técnicas, al incorporar la privacidad en la arquitectura misma de los sistemas, permiten trascender la aparente dicotomía entre transparencia y confidencialidad, creando lo que podríamos denominar “sistemas de transparencia selectiva” que revelan su funcionamiento general sin comprometer datos sensibles específicos.

Sin embargo, existen diversos marcos regulatorios equilibrados que ofrecen una perspectiva jurídica.

La conciliación entre transparencia algorítmica y privacidad diferencial requiere marcos regulatorios que superen el enfoque binario (todo público versus todo confidencial) para adoptar aproximaciones matizadas y contextuales. Tres principios fundamentales podrían orientar esta regulación equilibrada.

Primero, la proporcionalidad contextualizada: el nivel de transparencia requerido debe ser proporcional a la sensibilidad de la decisión algorítmica y su impacto en derechos fundamentales. Una aproximación de este tipo la encontramos en el recién aprobado *AI Act* europeo (2024), que establece “categorías diferenciadas de sistemas algorítmicos según su nivel de riesgo, con requisitos de transparencia progresivamente más

²¹ HINTON, G; VINYALS, O & DEAN, J. (2023). Distilling the Knowledge in a Neural Network. NIPS Deep Learning Workshop, 23 (4), pp. 1-9.

estrictos conforme aumenta el impacto potencial”²². Así, mientras que un algoritmo de recomendación musical estaría sujeto a requisitos mínimos de explicabilidad, un sistema de evaluación crediticia o diagnóstico médico enfrentaría estándares más rigurosos. Esta aproximación escalonada evita tanto la sobre-regulación que podría asfixiar la innovación como la infra-regulación que dejaría desprotegidos derechos fundamentales.

Segundo, la rendición de cuentas por diseño: los sistemas algorítmicos deberían ser conceptualizados desde su fase inicial para facilitar la auditoría externa sin comprometer datos sensibles. Este principio, inspirado en el concepto de “*privacy by design*” popularizado por Ann Cavoukian, requeriría que los desarrolladores implementen mecanismos de “trazabilidad selectiva” que permitan reconstruir el proceso decisorio en casos específicos sin exponer el conjunto completo de datos o parámetros. La implementación más avanzada de este concepto la encontramos en el “*Algorithmic Impact Assessment*” obligatorio para todas las decisiones automatizadas en el sector público canadiense desde 2021, que requiere “documentar exhaustivamente las consideraciones de diseño, fuentes de datos y mecanismos de mitigación de sesgos antes de la implementación de cualquier sistema algorítmico de toma de decisiones” (Government of Canada, 2023)²³.

Tercero, la supervisión independiente especializada: la creación de órganos técnicos con competencias específicas para auditar algoritmos críticos bajo estrictas normas de confidencialidad.

La experiencia internacional más cercana a este modelo la encontramos en el *Norsk Råd For Digital Etikk* (NORDE) con su proyecto de investigación “*Etisk Risikovurdering av KI i Praksis*” (ENACT), lanzado en 2023. ENACT

²² European Parliament and Council. (2024, 12 de julio). Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act). Official Journal of the European Union, L 2024/1689.

²³ Government of Canada. (s. f.). Algorithmic Impact Assessment tool. Treasury Board of Canada Secretariat. Recuperado el 9 de mayo de 2025, de <https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/responsible-use-ai/algorithmic-impact-assessment.html>

desarrolla una metodología de “trazabilidad selectiva” que permite reconstruir decisiones de sistemas de IA de alto riesgo sin exponer la totalidad de los datos o parámetros internos, mediante acuerdos de confidencialidad con expertos externos y garantizando así tanto la protección de la propiedad intelectual como la posibilidad de auditorías independientes ²⁴.

Un enfoque regulatorio que integre estos tres principios permitiría equilibrar la necesaria rendición de cuentas democrática con la protección de intereses legítimos como la privacidad individual, la seguridad de los sistemas y los derechos de propiedad intelectual, reconociendo que la transparencia no es un valor absoluto sino contextual, cuya implementación debe adaptarse a las circunstancias específicas de cada caso.

V. Implicaciones para el Estado de Derecho en la Era Digital

La tensión entre transparencia algorítmica y privacidad diferencial trasciende lo meramente técnico para situarse en el núcleo de cómo conceptualizamos el Estado de Derecho en sociedades cada vez más mediadas por algoritmos. Podemos identificar al menos tres dimensiones fundamentales. En primer lugar, se encuentra la reconfiguración del principio de publicidad de las normas y actuaciones estatales, el cual es pilar fundamental del Estado de Derecho moderno, y enfrenta una transformación radical. Si, como afirmaba Bobbio²⁵, “la democracia es el gobierno del poder público en público” ¿cómo reconciliar este principio con la creciente delegación de decisiones públicas a sistemas algorítmicos opacos?

La respuesta podría encontrarse en lo que podríamos denominar una “publicidad adaptativa”: un modelo que garantice la visibilidad y comprensibilidad de las decisiones algorítmicas para los ciudadanos afectados, aunque el mecanismo técnico específico permanezca parcialmente reservado por razones de seguridad, eficacia o protección de datos.

²⁴ Norsk råd for digital etikk. (2023). Etisk risikovurdering av KI i praksis. NORDE. Recuperado el 9 de mayo de 2025, de <https://www.norde.digital/>

²⁵ BOBBIO, N. (2013). *Democracia y secreto*. Fondo de Cultura Económica, pp. 37-38.

En segundo lugar, se encuentra el derecho al debido proceso, entendido tradicionalmente como la posibilidad de conocer y controvertir las pruebas y razonamientos que fundamentan una decisión, requiere una reconceptualización en entornos algorítmicos. El desafío consiste en definir qué constituye una “explicación suficiente” cuando el proceso decisorio involucra sistemas de aprendizaje automático con millones de parámetros.

Un enfoque prometedor podría ser el desarrollo de “proxies explicativos”: representaciones simplificadas pero fieles del razonamiento algorítmico, que permitan a ciudadanos sin conocimientos técnicos avanzados comprender y potencialmente impugnar decisiones automatizadas que les afectan.

Finalmente, la equidad procesal —entendida como igualdad de armas entre las partes— adquiere nuevas dimensiones cuando una de las “partes” es un algoritmo. La asimetría de conocimiento entre los desarrolladores del sistema y los ciudadanos afectados por sus decisiones crea un desequilibrio fundamental que amenaza la legitimidad del proceso.

Para mitigar esta asimetría, podría contemplarse el desarrollo de “defensores algorítmicos públicos”: expertos técnicos independientes que asistan a ciudadanos en la comprensión e impugnación de decisiones automatizadas, similar a cómo los defensores públicos proporcionan asistencia legal a quienes no pueden costearla.

VI. Conclusiones: Hacia un Nuevo Equilibrio

La opacidad algorítmica, como hemos demostrado, compromete principios fundacionales del Estado de Derecho. Cuando COMPAS clasifica a un acusado como “alto riesgo” de reincidencia sin revelar su metodología, o cuando un algoritmo crediticio rechaza un préstamo sin explicación substantiva, estamos ante un retroceso inquietante a formas pre-modernas de poder: decisiones que afectan derechos fundamentales pero que permanecen inmunes al escrutinio racional.

Por otra parte, la privacidad diferencial ofrece una respuesta técnicamente sofisticada al problema de protección de datos, pero genera sus propias problemáticas.

Las aproximaciones intermedias que hemos identificado —explicabilidad por capas, técnicas avanzadas de privacidad, y marcos regula-

torios equilibrados— ofrecen caminos prometedores, pero requieren una implementación cuidadosamente calibrada. La propuesta de “explicabilidad por capas” encuentra un paralelismo interesante en el principio de “defensa en profundidad” utilizado en seguridad nuclear: múltiples barreras de protección con diferentes funciones y niveles de acceso.

En el ámbito regulatorio, el recién aprobado *AI Act* europeo (2024) representa el intento más ambicioso hasta la fecha de abordar esta tensión. Su enfoque basado en riesgos, que establece requisitos de transparencia proporcionalmente más estrictos según el impacto potencial del sistema algorítmico, ofrece un marco conceptual valioso. Sin embargo, este modelo enfrenta desafíos significativos en su implementación práctica: la categorización de sistemas por nivel de riesgo presupone una capacidad evaluativa que, paradójicamente, requiere cierto grado de transparencia previa. Estamos ante lo que podríamos denominar una “circularidad regulatoria”: para determinar qué nivel de transparencia exigir a un algoritmo, necesitamos primero comprender su funcionamiento con suficiente detalle para evaluar sus riesgos potenciales.

Las implicaciones para el Estado de Derecho en la era digital son profundas y multifacéticas. La reconfiguración del principio de publicidad requiere lo que podríamos denominar una “transparencia adaptativa”: no necesariamente la exposición completa de cada parámetro técnico, sino la garantía de que las decisiones algorítmicas sean comprensibles y contestables por los ciudadanos afectados.

La búsqueda de equilibrio entre transparencia algorítmica y privacidad diferencial es, en última instancia, una manifestación específica de la tensión perenne entre valores democráticos fundamentales. Al igual que la libertad de expresión debe equilibrarse con la protección de otros derechos, o la seguridad nacional con las libertades civiles, la sociedad digital deberá encontrar su propio punto de equilibrio entre la necesaria transparencia de los sistemas que toman decisiones críticas y la imprescindible protección de la privacidad individual en una era de dataficación masiva y capitalismo de vigilancia.

El desafío para juristas, tecnólogos, filósofos y ciudadanos no consiste meramente en encontrar un punto de equilibrio momentáneo, sino en desarrollar marcos conceptuales, técnicos y normativos que permitan una recalibración continua y responsiva. En palabras de Lawrence Lessig, “el código es ley” —la arquitectura tecnológica incorpora valores

y distribuye poder — pero, complementariamente, necesitamos asegurar que la ley pueda efectivamente gobernar el código, estableciendo los principios fundamentales que deben orientar el diseño tecnológico en una sociedad democrática.

Al final, la tensión aparentemente irresoluble entre algoritmos opacos y privacidad diferencial nos recuerda que la tecnología nunca es neutral. Cada decisión de diseño algorítmico, cada implementación de mecanismos de privacidad, cada marco regulatorio refleja y refuerza determinadas concepciones sobre la relación entre individuo, sociedad y Estado. En la era de la hiperconectividad digital, estos sistemas técnicos se convierten en infraestructuras de gobernanza de facto, con profundas implicaciones para el ejercicio de derechos fundamentales y la distribución de poder social.

Es alentador observar cómo, mientras debatimos estos desafíos aparentemente irresolubles a nivel teórico, la industria tecnológica ya avanza en implementaciones concretas que buscan el equilibrio que hemos analizado. En octubre de 2024, Google liberó PipelineDP4J, una biblioteca de código abierto que implementa privacidad diferencial en Java, extendiendo sus soluciones de privacidad mejorada a “más de la mitad de los desarrolladores a nivel mundial” al incorporar ahora Python, Java, Go y C++ entre sus opciones²⁶. Lo particularmente significativo de esta iniciativa no es solo la democratización de estas herramientas matemáticas sofisticadas, sino su enfoque dual: por un lado, facilita el acceso a técnicas que protegen datos individuales mientras permiten análisis agregados valiosos; por otro, proporciona mediante DP-Auditorium mecanismos para verificar independientemente las garantías de privacidad ofrecidas, sin necesidad de acceso a las propiedades internas de las aplicaciones. Este desarrollo cristaliza perfectamente el equilibrio dinámico entre utilidad de los datos y protección de la privacidad que hemos propuesto como fundamento para reconciliar valores aparentemente antagónicos. Más que un mero avance técnico, representa la materialización práctica de los principios de “transparencia selectiva” y “rendición de cuentas por diseño” que hemos identificado como esen-

²⁶ GUEVARA, M. (2024, 31 de octubre). Open sourcing our Java-based differential privacy library. Google Privacy & Security Blog. Recuperado el 12 de mayo de 2025, de <https://blog.google/technology/safety-security/open-sourcing-our-java-based-differential-privacy-library/>

ciales. Demuestra que el camino hacia la coexistencia de algoritmos auditables y privacidad robusta no es una aspiración abstracta, sino una realidad emergente impulsada por implementaciones concretas que permiten extraer valor analítico de los datos sin comprometer derechos fundamentales de privacidad.

La disyuntiva no es, por tanto, meramente técnica sino profundamente política y ética: ¿qué tipo de sociedad queremos construir a través de nuestras decisiones tecnológicas? Una respuesta responsable exige trascender tanto el determinismo tecnológico como la regulación reactiva, adoptando en su lugar un enfoque de “gobernanza anticipatoria” que integre consideraciones éticas, sociales y democráticas desde las etapas iniciales del diseño tecnológico. Solo así podremos asegurar que la revolución algorítmica fortalezca, en lugar de socavar, los principios fundamentales del Estado de Derecho y la dignidad humana en el siglo XXI.

Del acoso al abuso en el marco de la violencia sexual ejercida en el ciberespacio

Pablo Jesus Juan Cortez Alvarez Cier*

Resumen.- El autor reflexiona sobre la estructura típica del delito de proposiciones a menores de edad con fines sexuales por medios tecnológicos (*child grooming*) con el fin de dar respuesta a diversas problemáticas, en especial aquella referida a si los supuestos donde el *groomer* consigue la finalidad sexual pretendida deberán ser tratados con las reglas de un concurso de leyes o de un concurso de delitos.

Palabras clave.- Ciberacoso - concurso de leyes - concurso de delitos.

Abstract.- The author reflects on the typical structure of the crime of child grooming in order to respond to various issues, especially the one referred to whether the cases where the groomer achieves the intended sexual purpose should be treated with the rules of a concurrence of laws or a concurrence of crimes.

Keywords.- Child grooming - concurrence of laws - concurrence of crimes.

* Estudiante de sexto año de Derecho en la Universidad Nacional Mayor de San Marcos. Asistente de cátedra en los cursos de Derecho Procesal Penal I y Derecho Penal II en la misma casa de estudios. Miembro principal del Taller de Dogmática Penal - UNMSM. Miembro fundador y coordinador general del Círculo de Estudios de Derecho Informático “Rocío del Pilar Rondinel Sosa” - UNMSM.

Nota: Artículo homenaje a mi hermano Joseph Maykol Rolando Rodríguez Chávarry, que en paz descansa.

I. Introducción

En la literatura criminológica se ha estudiado por ya buen tiempo un preocupante fenómeno o problema social que ha recibido diversas denominaciones tales como *grooming*, *child grooming*, *online grooming*, ciber*grooming*, ciberacoso sexual, acoso en línea, entre otras; términos pasibles de ser definidos, de acuerdo con Webster et al.¹ como el proceso donde una persona se hace amiga de un joven en línea para facilitar el contacto sexual online y/o un encuentro presencial de la misma índole con el menor, cuya finalidad consistirá en cometer abusos sexuales.

La gravedad de estos comportamientos dirigidos contra menores, provocó que el legislador peruano tipificara en el artículo 5 de la Ley 30096 “Ley de Delitos Informáticos”, el tipo penal de proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos, que sanciona con una pena privativa de libertad de entre seis y nueve años, al que valiéndose de internet u otro medio análogo, contacte con un menor de catorce años con el fin de solicitar u obtener de él material pornográfico, o para proponerle realizar cualquier acto de connotación sexual con él o con un tercero. El segundo párrafo del mismo artículo, por su parte, prevé una penalidad de menor gravedad –de tres a seis años de cárcel– en el supuesto de que la víctima tenga entre catorce y menos de dieciocho años de edad siempre que medie engaño. A efectos de un análisis dogmático más riguroso y pormenorizado, nos centraremos en adelante solamente en el primer párrafo y descartaremos también el estudio de la finalidad de obtener material pornográfico.

Con esta precisión, tenemos que de la redacción del tipo penal in comento, se desprende su naturaleza como un delito de tendencia interna trascendente, ya que requiere que el sujeto activo ejecute la conducta típica con cierta motivación específica. Estamos hablando pues, para el caso del *child grooming*, de un delito mutilado en dos actos donde el primero de ellos consiste en contactar con un menor de edad, y el segundo en llevar a cabo algún acto de carácter sexual con él, donde solo la ejecución del primer acto, aunada a la motivación de cometer el segundo, será necesaria

¹ WEBSTER, S., DAVIDSON, J. BIFULCO, A., GOTTSCHALK, P., CARETTI, V., PHAM, T., GROVE-HILLS, J., TURLEY, C., TOMPKINS, C., CIULLA, S., MILAZZO, V., SCHIMMENTI, A. Y CRAPARO, G. (2012). *European online grooming project - Final Report.*, pp. 5.

para su punibilidad, no siendo exigible que efectivamente se cumpla con tal finalidad. De ahí que para la doctrina predominantemente mayoritaria nos encontremos ante un delito de peligro, donde no es necesaria la efectiva lesión del bien jurídico tutelado para que se configure el tipo.

A raíz de dicha realidad surgen las primeras problemáticas de la presente investigación, traducibles en las siguientes interrogantes: ¿De qué manera se justifica la incoación del ius puniendi estatal para la persecución de comportamientos donde aún no se ha lesionado como tal el bien jurídico protegido? Siendo el bien jurídico que se pretende tutelar en el *child grooming*, la indemnidad sexual del menor, ¿esta no es acaso ya lesionada con la mera proposición sexual?

Asimismo, si producto del ciberacoso se llegare a consumir la finalidad de perpetrar actos sexuales, como bien podrían ser la violación sexual o los tocamientos indebidos contra menor de edad (artículos 173 y 176-A del Código Penal peruano), ¿estaríamos hablando de un concurso de leyes, donde solamente se imputarían tales actos sexuales y no el *online grooming*? ¿O estos supuestos deberían ser tratados como un concurso real y, en consecuencia, atribuir responsabilidad por ambos delitos? La resolución de los problemas planteados hasta el momento se justifica en la necesidad de contar con parámetros claros de las reglas concursales en el delito de *child grooming*, dada la poca atención que ha recibido en el ámbito nacional por la doctrina y jurisprudencia.

Cabe precisar que es justamente tal escaso desarrollo jurisprudencial y dogmático peruanos, lo que nos empuja a recurrir en la presente investigación, en función a una metodología de derecho comparado, a las fuentes del derecho español, las cuales, además de haber abarcado con mayor rigurosidad y amplitud el delito sub examine, resultan completamente compatibles con nuestro derecho nacional, no solo por su cercanía al pertenecer a la misma tradición jurídica europeo-continental en general, sino específicamente por las similitudes existentes –con la salvedad de las particularidades en ambos regímenes que se dejarán claras en el artículo– entre los preceptos jurídicos que regulan el *child grooming* y las reglas concursales.

De esta manera, en aras de resolver las problemáticas planteadas con base en una estructura ordenada de investigación, en el presente artículo se realizará primero un estudio preliminar de la tipicidad y naturaleza del delito de proposiciones a menores de edad con fines sexuales por medios

tecnológicos. Posteriormente, se procederá con el análisis de la legitimidad de este tipo penal en el ordenamiento jurídico peruano, luego, se expondrán las tesis dogmáticas existentes respecto de los conflictos concursales que surgen cuando el groomer alcanza la finalidad sexual pretendida ya sea a través de tocamientos indebidos o del acceso carnal. Finalmente, se tomará postura respecto de si en los supuestos de progresión delictiva donde el groomer consigue su cometido, y tanto el bien jurídico afectado como el sujeto pasivo son los mismos, deberán ser tratados en base a las reglas de un concurso de leyes o de un concurso de delitos.

ii. Tipicidad y naturaleza del *child grooming* como delito de peligro o de lesión

El bien jurídico protegido en el primer párrafo del artículo 5 de la Ley de Delitos Informáticos es la indemnidad sexual entendida como el normal y correcto desarrollo de la sexualidad del menor de catorce años sin interferencias ajenas que puedan perturbarlo. No es pues la libertad sexual la que se pretende tutelar en estos casos, sino la indemnidad o intangibilidad sexual, de ahí que la existencia de consentimiento para el contacto sexual por parte de la víctima no constituye una causal de atipicidad en los delitos sexuales cometidos contra menores de catorce años.

En ese sentido se pronuncia la Corte Suprema en el RN 2321-2014, FJ 7, donde precisa que el bien jurídico tutelado en el delito de violación previsto en el artículo 173 del Código Penal, es la indemnidad sexual del sujeto pasivo, puesto que en el caso objeto del recurso, la víctima tenía once años de edad cuando se cometió la violación sexual, por ende, en ese momento no contaba con capacidad jurídica para disponer de su sexualidad libremente, es decir, el hecho de que la menor haya consentido o no las relaciones sexuales con el condenado resulta totalmente irrelevante.

Ahora bien, ¿en el tipo penal de *child grooming* se pretende sancionar la lesión o la puesta en peligro de la indemnidad sexual del menor? O lo que es lo mismo, ¿estamos hablando de un delito de lesión o de peligro ya sea abstracto o concreto? Para algunos autores como Villacampa Estiarte², se trataría de un delito de peligro abstracto en tanto que a

² VILLACAMPA, C. (2015). *El delito de online child grooming o propuesta sexual telemática a menores*. Valencia: Tirant lo Blanch, pp. 158.

través de su incriminación se ha buscado adelantar las barreras punitivas a un estadio previo a la ejecución de comportamientos directamente lesivos contra la indemnidad sexual, como el abuso o la agresión sexual emprendidos contra aquellos que no ostentan la edad mínima para la autodeterminación sexual.

De opinión similar es Muñoz Conde³, para quien, en tanto que el embaucamiento de menores con fines sexuales constituye un acto preparatorio⁴ de otros delitos contra la indemnidad sexual, es correcto adoptar la postura del peligro abstracto a pesar de requerirse en el ordenamiento penal español «actos materiales encaminados al acercamiento», toda vez que no resulta tan fácil determinar si tal acercamiento se emprende con el ánimo de realizar algún delito. Por el contrario, el Tribunal Supremo español se ha decantado por la tesis del peligro concreto, en tanto que, de acuerdo con el FJ 1 de la STS 97/2015, el tipo penal requiere de la existencia de un menor de edad y de la ejecución de actos materiales dirigidos al acercamiento sexual.

A decir de Górriz Royo⁵, parece entenderse que esa “materialidad” haría necesaria la prueba de actos que acrediten que la lesión de la indemnidad sexual es posible en el caso concreto. Esto último fungiría como argumento a favor de la tesis del peligro concreto, ya que en esta clase de delitos, tal como los comprende Mezger⁶, se requiere no solo la realización de la conducta prevista en el tipo penal, la cual sería suficiente para afirmar la condena en los delitos de peligro abstracto puesto que se presume como generalmente peligrosa, sino que resulta exigible además que se demuestre en el supuesto particular la efectiva y real puesta en peligro del bien jurídico protegido en el tipo correspondiente.

³ MUÑOZ, F. (2014). *Derecho Penal Parte Especial* (2ª. ed.). México: Tirant lo Blanch, pp. 230.

⁴ En el mismo sentido, ORTS, E., VIVES, T., CARBONELL, J., GONZÁLEZ Y MARTÍNEZ-BUJÁN. (2010). *Derecho Penal Parte Especial*. Tirant lo Blanch (3ª. ed.). Valencia: Tirant lo Blanch, pp. 269.

⁵ GÓRRIZ, E. (2016). “On-line child grooming” en *Derecho penal español*. InDret, (3), 1-47, pp. 30.

⁶ MEZGER, E. (1958). *Derecho Penal*. Libro de Estudio Parte General. Buenos Aires: Editorial Bibliográfica Argentina, pp. 150.

Tal argumento sobre la existencia de “actos materiales” para afirmar la naturaleza del *child grooming* como un delito de peligro concreto, supone un asunto más controvertido en el ámbito jurídico peruano, pues nuestra fórmula de tipicidad es mucho menos específica, veamos la comparación del tipo sub examine en los ordenamientos español y peruano:

Art. 183. 1 del Código Penal español	Art. 5 de la Ley peruana 30096
El que, a través de internet, del teléfono o de cualquier otra tecnología de la información y la comunicación contacte con un menor de dieciséis años y proponga concertar un encuentro con el mismo a fin de cometer cualquiera de los delitos descritos en los artículos 181 y 189, siempre que tal propuesta se acompañe de <u>actos materiales encaminados al acercamiento</u> [...].	El que a través de internet u otro medio análogo contacta con un menor de catorce años [...] <u>para proponerle</u> llevar a cabo cualquier acto de connotación sexual con él o con tercero [...].

Vemos pues que mientras el código español prevé tres conductas para configurarse el tipo penal (contactar, proponer y actos materiales), nuestra Ley de Delitos Informáticos únicamente requiere la conducta típica «contactar» por medios telemáticos, mientras que la finalidad sería la proposición sexual. De cualquier forma, no hay que olvidar que por más reprochables y deleznable que nos parezcan las intenciones de estos sujetos, de acuerdo a la *máxima cogitationis poenam nemo patitur*, el Derecho Penal no sanciona meros pensamientos, por lo que es necesario que la finalidad sexual se manifieste en el contacto con el menor o en las proposiciones que se le hicieren a efectos de obtener una condena por este delito, son a fin de cuentas cuestiones que obedecen más que todo al ámbito procesal y a la lógica de la actividad probatoria. Así pues, De la Mata Barranco⁷ señala, dentro de su marco jurídico español, que hasta que la intención sexual “no se manifieste en sucesivas propuestas de encuentro, impedirá la sanción por el delito”.

⁷ DE LA MATA, N. (2017). El contacto tecnológico con menores del art. 183 ter 1 CP como delito de lesión contra su correcto proceso de formación y desarrollo personal sexual. Revista Electrónica de Ciencia Penal y Criminología., pp. 16.

Volviendo al punto de partida sobre la naturaleza del delito de *child grooming*, recordemos que si bien la redacción hecha por el legislador peruano es mucho más amplia que la española, sin requerir por tanto la existencia de actos materiales encaminados al acercamiento, de todas formas se exige la concurrencia de un menor de catorce años sobre el que recae la acción típica, entonces el peligro parece ser más cercano a un efectivo resultado de lesión a diferencia de lo que ocurre en un delito de peligro abstracto en puridad de términos.

Además, si como ha admitido ya la jurisprudencia española y argentina⁸, los tocamientos indebidos y accesos carnales como finalidades sexuales pretendidas por el *groomer* pueden realizarse a gran distancia por medios telemáticos⁹, entonces la lejanía entre el peligro representado por la proposición sexual y el eventual resultado de lesión concretado en la realización de actividades sexuales se reduce significativamente, por lo que hablar de un peligro concreto ya no resultaría tan descabellado, aunque de cualquier forma el artículo 5 de la Ley 30096 no requiere que en efecto se haya expuesto a un peligro real la indemnidad sexual del menor, sino que parece ser que el mero contacto se presume ya peligroso, razón por la que se asemejaría también su estructura a la de un tipo de peligro abstracto. En fin, dado el escaso desarrollo jurisprudencial que se ha hecho sobre este delito en el Perú, no es posible dar más aproximaciones que las ya hechas en abstracto, pero lo que sí queda claro es su peculiar estructura típica que sin duda merece mayor atención por parte de la doctrina y judicatura.

Por último, merece la pena resaltar una postura ubicada, con motivos justificados, en el polo opuesto de las dos anteriores. El ciberacoso a menores no es pues, para algunos, un delito de peligro, sino de lesión, ya que el contacto con la víctima a través de medios telemáticos y

⁸ Véase la Sentencia 203 del Expediente 2469171 emitida por el Tribunal Superior de Córdoba y la STS 447/2021 emitida por el Tribunal Supremo español.

⁹ En contraposición a esta premisa, algunos sostienen que la finalidad pretendida por el *groomer* debe ser un encuentro sexual presencial, aunque ya la jurisprudencia española en la STS 376/2023 haya admitido la virtualidad del encuentro. Véase Carrasco Andrino, M. (2024). Agresiones sexuales sobre menores de 16 años (II). Los delitos de proposición sexual telemática y de embaucamiento, y la cláusula del consentimiento del art. 183 bis CP. En *Tratado de Derecho Penal Español Parte Especial (I) Delitos contra las personas*. Dir. F. Álvarez García, pp. 1357-1359.

propuestas con fines sexuales perturba ya el normal procedimiento de descubrimiento o desarrollo de la sexualidad, es decir, se vulnera con la acción típica la indemnidad sexual del menor. Para esta línea de pensamiento, la libertad sexual podrá peligrar cuando se encuentre en riesgo una toma de decisión fundamentada en un consentimiento válido; en esa línea, conforme a De la Mata Barranco, “en el caso de los menores cuando el proceso que le permite poder llegar a ejercer esa libertad en madurez quiebra [...] no podemos hablar de peligro sino de lesión”¹⁰. Así pues, según el autor citado, el contacto con intenciones sexuales manifestadas altera la percepción del menor respecto de su sexualidad, haciendo que aquél la considere como algo secreto, oscuro o turbio.

Consideramos que la tesis de lesión, aunque minoritaria, es la que se condice más con la realidad, toda vez que la indemnidad sexual del menor abarca no solo su esfera somática, sino también la psicosexual, la cual se ve precisamente perturbada ya a partir de determinados contactos tecnológicos con fines sexuales con los groomers, lo que no quiere decir que, dado el extenso abanico de posibilidades que tiene el ciberacosador en su modus operandi –por ejemplo mediante el contacto “amigable” con el menor a través de videojuegos¹¹–, “[...] no quepa plantear supuestos de únicamente peligro, sino de entender que (aun no siempre) esa relación asimétrica menor-adulto de contenido sexual (cuando el mismo esté presente) facilitada tecnológicamente excede la frontera del mero peligro”¹². Dicho ello, se puede arribar también a la idea concluyente de que el ciberacoso a menores constituye un adelantamiento de las barreras punitivas estatales que, en relación con la eventual comisión de los delitos sexuales tradicionales como el acceso carnal o los actos libidinosos, implicaría un supuesto de progresión delictiva.

¹⁰ De la Mata Barranco, N. (2017). El contacto tecnológico con menores del art. 183 ter 1 CP como delito de lesión contra su correcto proceso de formación y desarrollo personal sexual. *Revista Electrónica de Ciencia Penal y Criminología*., pp. 19.

¹¹ Para mayor información, véase: Rojas Marcelo, J. (2024). Child grooming en videojuegos en línea: Un análisis de la ciberdelincuencia y la protección de los niños en América Latina. *Lacnic*.

¹² DE LA MATA, N. (2017). El contacto tecnológico con menores del art. 183 ter 1 CP como delito de lesión contra su correcto proceso de formación y desarrollo personal sexual. *Revista Electrónica de Ciencia Penal y Criminología*, (19-10), 1-28, p. 19. En respaldo de esta idea: CINOSI, M. (2023). Online child grooming en España: análisis del tipo penal a través de la teoría del delito. *Rev. Boliv. de Derecho*., pp. 261.

III. Legitimidad en el ordenamiento penal

Ya sea que optemos por una u otra tesis, como quiera estamos ante un adelantamiento de la protección penal hacia estadios previos donde, o bien no se ha lesionado todavía la indemnidad sexual (tesis del peligro), o bien se ha lesionado (tesis de lesión), pero con una intensidad muy inferior a la existente en otros delitos sexuales contra menores de edad que pretende perpetrar el *groomer* a través del contacto inicial por vías telemáticas (acceso carnal, tocamientos indebidos, etc.). ¿Qué justifica entonces este adelantamiento a efectos de considerar legítimo el tipo penal *sub examine*? Veamos.

Hay quien fundamenta la punición de estos comportamientos en base a la moderna categoría creada por el insigne penalista de la Universidad de Bonn Günter Jakobs, el Derecho Penal del Enemigo. En esa línea de ideas se enmarca Granja¹³, para quien el *groomer*, pederasta o minotauro digital, debe ser tratado como enemigo en términos jakobsianos; en esa inteligencia, el *groomer* constituye un foco de peligro que debe ser neutralizado mediante el anticipo de punibilidad, toda vez que la peligrosidad es tal que no podría recibir el mismo tratamiento jurídico-penal que el desliz normativo en el que incurre alguien que simplemente hurta una botella de vino y, por ende, conserva su estatus de ciudadano.

El profesor Pedro Javier Granja hace referencia allí a dos tipos de normas que existen en los ordenamientos penales actuales: i) Normas de derecho penal del ciudadano y ii) normas de derecho penal del enemigo. Las primeras tienen como destinatario simplemente a aquellos delincuentes tradicionales que han incurrido en algún desliz normativo como pueden serlo ladronzuelos, homicidas, estafadores, entre otros. Las segundas, por otra parte, están dirigidas a delincuentes especialmente peligrosos que se apartan frontal y directamente de la norma de forma duradera, el ejemplo clásico son los miembros de organizaciones criminales. En ese sentido, señala Bastida Freixedo¹⁴, mientras que el ciudadano delincuente habla nuestro idioma, aunque erróneamente, y la pena pretende corregirlo reafirmando la vigencia de la norma, el enemigo, por

¹³ GRANJA, P. (2021). “Gromming”: el minotauro en internet. El derecho penal del enemigo frente al pederasta de la era digital. *Derecho Penal y Criminología*, pp. 98.

¹⁴ Como se citó en Jakobs, G. (2015). *El lado comunicativo y el lado silencioso del derecho penal*. Editores del Centro, p. 69.

otra parte, habla una lengua totalmente distinta y se niega a aprender la nuestra.

Ahora bien, ya hemos tenido la oportunidad de discurrir sobre el derecho penal del enemigo en otra investigación¹⁵, sin embargo, conviene hacer un par de acotaciones a efectos de un análisis más integral del caso concreto. Según Polaino-Orts¹⁶, discípulo directo de Jakobs, se pueden enumerar las siguientes tres características propias de un Derecho Penal del Enemigo: i) El adelantamiento del castigo a estadios anteriores a los que suele sancionar el Derecho penal del ciudadano; ii) la restricción de la libertad, impidiendo al enemigo lo que en otras circunstancias sería el ejercicio legítimo de un derecho y iii) la falta de reducción de pena de manera proporcional a la anticipación de punibilidad.

El primer párrafo del artículo 5 de la Ley 30096, como ya quedó demostrado, evidentemente constituye un supuesto de adelantamiento de la represión penal pues sanciona actos preparatorios de otros delitos contra la indemnidad sexual. Asimismo, se restringe la libertad de relacionarse e interactuar con otras personas en el ámbito privado del internet u otros medios análogos puesto que esa interacción está impregnada de fines perversos para con menores de edad. Por último, la pena con la que se sanciona el *grooming* tiene un marco abstracto de seis a nueve años, lo que sí resulta proporcionalmente menor que los tocamientos indebidos (nueve a quince años) o el acceso carnal a menor de catorce años (cadena perpetua).

Así pues, a pesar de no cumplirse a cabalidad con la última característica, el tipo penal referido guarda gran parte de la esencia de una norma de derecho penal del enemigo, siendo que este y su represión se enfoca más en los hechos futuros, esto es, lo que pueda cometer el autor (en el caso del *groomer*, lograr alcanzar las respectivas finalidades sexuales), que en lo que en realidad ya hizo. De cualquier forma, lo dicho hasta aquí es más que todo de un carácter descriptivo y no prescriptivo, por lo que

¹⁵ Véase Cortez Alvarez Cier, P. (2024). "Criterios claves para la determinación del peligro de fuga por la pertenencia del imputado a una organización criminal". En *Gaceta Penal & Procesal Penal*, (175), 72-84.

¹⁶ Polaino-Orts, M. (2011). Verdades y mentiras en el Derecho Penal del Enemigo. *Revista de la Facultad de Derecho y Ciencias Sociales y Políticas*, 5(9), 417-454, pp. 429-430.

no serviría tanto para fundamentar el adelantamiento de las barreras punitivas, lo que sí es de utilidad para los efectos señalados es responder a la pregunta de cuándo es legítimo considerar enemigo a un individuo, en palabras de Jakobs¹⁷:

Si se observa qué es aquello -más exactamente: quiénes son aquellos- contra lo(s) que se pretende «luchar», se constata que se trata de individuos que **en su actitud (delitos sexuales)**, en su vida económica (criminalidad económica, relativa a las drogas y otras modalidades de criminalidad organizada) o por su imbricación en una organización criminal (terrorismo, criminalidad organizada) **se han apartado, probablemente, de modo permanente, pero, en todo caso, con cierta seriedad del Derecho**, dicho de otro modo: que **no prestan la garantía cognitiva mínima** que es imprescindible para ser tratado como persona en derecho.

Tal déficit de seguridad cognitiva ocasionada por el enemigo se traduce en el desvalor social de la conducta que, a su vez, fundamenta su punibilidad. Ahora bien, si el *groomer* puede ser considerado enemigo o no en términos jakobsianos amerita de un análisis dogmático sustantivo más amplio y de un estudio integral que implique también experiencia criminológica y aspectos penales adjetivos, lo que excede los objetivos de la presente investigación. Lo que sí me resulta meridianamente claro con lo expuesto hasta ahora es que la anticipación de la protección penal que encontramos en el delito de *child grooming*, se encuentra perfectamente justificada y legitimada en función a i) la importancia del bien jurídico protegido, ii) la multiplicidad de resultados lesivos contra la indemnidad sexual que se pueden desprender del grooming y, por último, iii) el uso de las TIC como herramientas idóneas para delinquir. Pasemos a explicar esto con mayor detenimiento.

Conforme a García Caveró¹⁸, es imperativa la respuesta penal ante actos de preparación cuando estos pretenden atentar contra un bien jurídico de elevada importancia para la sociedad y siempre que de aquel comportamiento se pueda desprender una multiplicidad de cursos lesivos. Estas dos razones dotan de un especial sentido delictivo a los actos preparatorios, haciéndoles perder la ambigüedad o equivocidad

¹⁷ JAKOBS, G. (2006). *La pena estatal: significado y finalidad*. CANCIO, M. y FEIJOO, B. (trads.). Madrid: Thomson Civitas, pp. 170.

¹⁸ GARCÍA, P. (2019). *Derecho Penal Parte General* (3ª. ed.). Lima: Ideas, pp. 457.

que han servido de fundamento para su impunidad. Ambos presupuestos concurren satisfactoriamente en el delito de *child grooming*. Por un lado, de aquel se pueden derivar una gran variedad de resultados lesivos contra la indemnidad sexual del menor de catorce años, de entre los cuales cabe resaltar los tocamientos indebidos, el acceso carnal o violación sexual, la obtención de pornografía infantil, entre otros.

Por otro lado, es innegable la relevancia del bien jurídico “indemnidad sexual” siendo este un presupuesto para que los menores de catorce años desarrollen una sexualidad saludable y, una vez superado ese límite etario, dispongan de ella libremente en condiciones adecuadas. Tales estados se encuentran vinculados **íntimamente con el proyecto de vida y el libre desarrollo de la personalidad, los cuales son unos de los fines máximos de la persona humana. Y, por si fuera poco, nuestra carta magna, la norma fundamental, la Constitución Política de 1993 consagra en su artículo 4° como objeto de protección especial al niño y al adolescente, son ellos pues el futuro de la sociedad, por lo que la tutela de sus bienes jurídicos personalísimos es una necesidad inaplazable.**

A tales motivos de punición se agrega el empleo de las tecnologías de la información y la comunicación. Como menciona Clough¹⁹, i) la tecnología facilita el contacto entre potenciales ofensores y víctimas en una magnitud colosal; ii) las TIC permiten a los delincuentes mantenerse en el anonimato otorgando mayores posibilidades de impunidad; iii) resulta mucho más simple borrar las huellas de la comisión de un crimen en el entorno digital que en el ámbito físico; iv) hay una ausencia de guardianes capaces de controlar el ciberespacio, volviéndose prácticamente tierra de nadie y planteando desafíos a la policía para la prevención e investigación del cibercrimen; entre otros factores que dificultan la persecución de estos delitos.

Estas características inherentes a las TIC vuelven al ciberespacio una fuente incalculable de riesgos, un lugar idóneo para la comisión de delitos. El ciberdelincuente puede emprender el contacto con fines sexuales con una infinidad de víctimas al mismo tiempo y evitar ser descubierto gracias al anonimato y escasas de control estatal que ofrecen

¹⁹ CLOUGH, J. (2015). *Principles of cybercrimen*. Cambridge University Press, pp. 5-8.

estos entornos digitales, lo cual deviene en una actuación a sobre seguro que no solo justifica el plus de desvalor social en los injustos agravados por utilizar tales tecnologías, sino que también fundamenta y legitima la respuesta penal anticipada en el delito de ciberacoso a niños, niñas y adolescentes.

IV. Cuestiones concursales por la consecución de la finalidad sexual

Entendido el *child grooming* como un delito mutilado en dos actos y de tendencia interna trascendente, no es necesario que se consiga la finalidad sexual específica para consumarse el tipo, bastará con la mera proposición a través de medios tecnológicos. No obstante, surge la duda respecto de cómo deberían tratarse en términos concursales los supuestos donde el *groomer* alcance la finalidad del contacto sexual con el menor de catorce años, esto es:

- Estaríamos hablando de un concurso de leyes donde solo tendría que imputarse el contacto sexual entre el agresor y la víctima (acceso carnal y tocamientos indebidos contra menores) por ser un supuesto de progresión delictiva donde el delito fin absorbe el desvalor social del delito medio; o
- Por el contrario, esta situación supondría un concurso de delitos donde la imputación incluye tanto el ciberacoso como la perpetración de actividades sexuales con el menor, en virtud de que el ciberacoso contiene un desvalor adicional consistente en el medio comisivo (TIC), y que no es abarcado por el delito sexual fin.

Para resolver esta controversia recurriremos a jurisprudencia española, lo cual no es ningún óbice para aplicar al ámbito nacional las conclusiones finales a las que lleguemos en base a ella, toda vez que nuestra normativa en materia concursal es bastante similar.

i. Supuesto de concurso de leyes

El concurso de leyes, también denominado concurso aparente de delitos, no cuenta con una regulación expresa en nuestro ordenamiento, sin embargo, posee su fundamento normativo en el principio de *non bis in idem* (artículo III del Título Preliminar del Código Procesal Penal peruano), que en pocas palabras proscribe sancionar dos veces por los mismos hechos. Así las cosas, el concurso de leyes surge cuando una

conducta puede subsumirse en varios tipos penales al mismo tiempo, pero que solo es punible por uno de ellos en la medida que únicamente este abarcaría el completo sentido delictivo del comportamiento.

De esta manera, si Juan mata a Alberto a cambio de dinero, su actuación calza tanto en el delito de homicidio simple, como en el delito de asesinato u homicidio calificado (artículos 106 y 108 del Código Penal), no obstante, solamente esta segunda figura es imputable a Juan, pues abarca el total desvalor social de los hechos, mientras que la primera omite el elemento de móvil de lucro. Imputar y condenar por ambos tipos penales vulneraría el principio referido al valorarse doblemente una misma conducta.

Ahora bien, debemos precisar que, en virtud del principio o criterio de subsidiariedad, existen ciertos tipos penales subsidiarios que solo se aplicarán cuando el hecho antijurídico no se encuentre abarcado por un tipo penal más estricto. Es lo que sucede, por ejemplo, con el delito de falsedad genérica (art. 438 del CP) como un tipo penal de recogida que solo podrá imputarse cuando el hecho punible no sea aprehendido por los demás delitos contra la fe pública. Esta relación de subsidiariedad también concurre entre las fases de realización de un delito donde la responsabilidad por un delito consumado se prefiere a la responsabilidad por tentativa del mismo, y esta última se prefiere ante la responsabilidad por el acto preparatorio si fuera punible por el ordenamiento penal²⁰.

Conforme a lo mencionado, Montserrat²¹ sindicada que entre el *child grooming* y los delitos sexuales que se llegaran a cometer gracias a él, existe un supuesto de progresión delictiva donde, si bien no hay unidad fáctica naturalísticamente hablando, sí concurre una unidad normativa del hecho, toda vez que el sentido delictivo del acto preparatorio se encuentra ya aprehendido por los delitos que lesionan directamente la indemnidad sexual del menor. Esto en base a dos razones: i) el *child grooming* es solamente un acto preparatorio que constituye el tránsito para la comisión del delito fin y ii) tanto el *grooming* como el abuso sexual de menores afectan un mismo bien jurídico, pero con una intensidad distinta.

²⁰ GARCÍA, P. (2019). *Derecho Penal Parte General* (3ª. ed.). Lima: Ideas, pp. 854-855.

²¹ MONTSERRAT, M. (2018). Propuesta para la interpretación de la cláusula concursal recogida en el artículo 183, ter 1 (Delito de Online Child Grooming). *R.E.D.S.*, pp. 145.

Sobre esta misma línea de pensamiento se erigen algunos pronunciamientos jurisprudenciales de España, que ven un concurso de normas o de leyes entre el *child grooming* y los delitos de los artículos 181 y 189 del Código penal español, es decir, allí donde la finalidad sexual del *groomer* es conseguida. Esta postura tiene su razón de ser, entre otras cosas, en que el Tribunal Supremo considera que: a) tanto el delito medio como el delito fin protegen un mismo bien jurídico, la indemnidad sexual (STS 97/2015); b) el inicio de la ejecución del abuso sexual entendido como delito de lesión, ya absorbe el desvalor del delito de peligro reflejado en el ciberacoso (STS 527/2015); y c) se trata de un supuesto de progresión delictiva donde el grooming es el acto preparatorio del abuso sexual (STS 864/2015).

ii. Supuesto de concurso de delitos

En el concurso de delitos el comportamiento o los comportamientos punibles son subsumibles en más de un tipo penal, la diferencia con el concurso de leyes radica en que en este caso sí resultará aplicable más de un tipo a efectos de determinar la pena. Existen dos clases de concurso de delitos según la normativa peruana, el real y el ideal (artículos 50 y 48 del Código Penal respectivamente), estableciéndose un tratamiento punitivo distinto para ambos casos; en el primero concurren varios hechos punibles que deben ser castigados independientemente, es decir, habrá tantos hechos como tipos aplicables, mientras que en el segundo existe un solo hecho al cual le son imputables más de un delito.

Para Aguado López²², cuando el *groomer* logra conseguir su finalidad sexual, habría concurso de normas si el bien jurídico puesto en peligro y finalmente lesionado es el mismo. Por el contrario, hablaremos de un concurso de delitos solo si los bienes jurídicos afectados son diferentes ya sea por pertenecer la indemnidad sexual a sujetos pasivos distintos –cuando se realiza la propuesta sexual a varios menores, pero no se llega a abusar de todos o se abusa solamente de uno de ellos–, o por lesionarse otros bienes jurídicos además de la indemnidad sexual, como la vida, la

²² AGUADO, S. (2020). *Las reformas proyectadas de los delitos contra la “indemnidad sexual” en las leyes integrales de libertad sexual y de protección de la infancia. Especial referencia a los delitos de “child grooming” y “sexting” (artículo 183 ter)*. En GONZÁLEZ, J. L., (dir.), *Estudios jurídicos en memoria de la profesora doctora Elena Górriz Royo*, Ed. Tirant Lo Blanch, Valencia, 2020, pp. 76.

salud, la intimidad, etcétera²³. En este último caso, subsiste cierto peligro hacia la indemnidad de los menores que justifica la aplicación conjunta del delito de peligro y el delito de lesión, habiendo tantos delitos de ciberacoso como menores contactados y solicitados que no terminan siendo abusados²⁴.

No obstante, algunas voces judiciales sostienen ya desde hace años que, entre el ciberacoso y el posterior abuso sexual, de llegarse a cometer, tendría lugar un concurso real inclusive si la indemnidad puesta en peligro y la finalmente lesionada es la misma. En un estudio reciente, Sánchez Vilanova²⁵ determinó que hubo un cambio de paradigma en la interpretación que la jurisprudencia española hacía sobre estas cuestiones concursales. Así, si inicialmente se optó por tratar a los supuestos mencionados como una relación de concurso de leyes –tal como se observó en el apartado anterior–, con la STS 777/2017 empezaron a interpretarse estos casos como un concurso real en algunas sentencias tanto en sede del Tribunal Supremo como en jurisprudencia menor²⁶.

Esta sentencia entendió que entre el ciberacoso y el abuso sexual existe una relación de acto preparatorio y delito fin, donde cada uno de ellos merecerán sus condenas respectivas por tratarse de un concurso real delitos. Para fundamentar su postura, el Tribunal Supremo trajo a colación el Pleno no Jurisdiccional de fecha 8 de noviembre de 2017, donde se acordó que el delito de *child grooming* y los delitos de lesión contra la indemnidad sexual eran totalmente compatibles al agregar a los comportamientos de agresión, abuso sexual, o creación de pornografía infantil, un plus de desvalor reflejado en el medio comisivo utilizado para el acercamiento al menor, a saber, las tecnologías de la información y la comunicación.

²³ En el mismo sentido la STS 109/2017, de fecha 22 de febrero 2017, fundamento jurídico tercero.

²⁴ VILLACAMPA, C. (2015). *El delito de online child grooming o propuesta sexual telemática a menores*. Valencia: Tirant lo Blanch, pp. 168.

²⁵ SÁNCHEZ, M. (2023). *Child grooming y concursos: evolución del tratamiento jurisprudencial en el ordenamiento jurídico español*. Política criminal., pp. 421.

²⁶ En el mismo sentido, la STS 158/2019; Audiencia Provincial de Girona, sentencia n.º 283/2020; Audiencia Provincial de Valladolid, sentencia 25/2021.

Y es que claro, esa relación de subsidiariedad en los grados de realización del delito que justifica en principio el concurso de leyes decae “cuando la preparación presenta elementos especiales que no quedan abarcados por la consumación”²⁷, toda vez que el abuso sexual posterior ya no abarcaría el total desvalor del acto preparatorio por no incluir a las TIC en su ejecución. Es innegable pues el potencial lesivo que traen consigo tales tecnologías y que ya fue explicado en líneas anteriores al referirnos a la investigación de Jonathan Clough y las características criminógenas del ciberespacio, como el favorecimiento del contacto con múltiples víctimas, el anonimato, la facilidad del borrado de huellas del delito, la ausencia de guardianes capaces, entre otras cualidades que fundamentan un desvalor adicional reprochable.

iii. Toma de postura

Resulta meridianamente claro que en los casos donde el bien jurídico afectado sea diferente, la aplicación conjunta del delito de peligro y el delito de lesión deberá tener lugar como concurso real de delitos. Por el contrario, si se trata de un mismo bien jurídico afectado en la progresión delictiva, en este caso la indemnidad sexual del menor contactado por internet y ulteriormente abusado, el debate se acrecienta de manera exponencial. En este estado de cosas, la doctrina mayoritaria sostiene que el peligro cede al convertirse en lesiones concretas de bienes jurídicos individuales, toda vez que aquel es el germen de estas, perdiendo su autonomía, por lo que el concurso de delitos no se aplica en los supuestos donde el peligro y la lesión son dos fases de un mismo comportamiento²⁸. Esta afirmación carece de relevancia si, como aquí, se opta por la tesis del delito de child grooming como un tipo penal de lesión de la indemnidad sexual, pues ya no estaríamos hablando de una lesión que absorbe el peligro, sino de dos lesiones de distinta intensidad que deberán ser evaluadas de manera independiente.

²⁷ JAKOBS, G. (1997). *Derecho Penal Parte General. Fundamentos y teoría de la imputación* (3ª. ed.). Madrid: Marcial Pons, pp. 1060.

²⁸ HERNÁNDEZ, J. (1994). Delitos de peligro con verificación de resultado ¿Concurso de Leyes? *Anuario de Derecho Penal y Ciencias Penales.*, pp. 139.

Así pues, De La Mata Barranco²⁹ señala certeramente que cuando el desvalor del comportamiento de aquel que se sirve de las TIC para contactar con el menor se entiende que queda absorbido por consumarse la finalidad sexual perseguida, y es suficiente la imputación por uno de los delitos en conflicto para aprehenderlo en su integridad, optar por el concurso de leyes es lo adecuado. Sin embargo, ello resulta inaceptable en supuestos donde el desvalor del grooming pueda ser independizado con claridad del posterior abuso sexual tentado o consumado. Refiere este mismo autor que hay una única indemnidad sexual que puede ser lesionada en distintas intensidades y momentos. A contrario sensu, ello comporta que “en aquellos casos en los que la conducta previa de grooming carezca de la suficiente gravedad para independizar el tipo, se tenga que proceder a apreciar un concurso de normas”³⁰.

Con todo lo dicho hasta aquí podemos afirmar que existen dos realidades palpables: i) en general, las tecnologías de la información y la comunicación aportan cierto grado de peligrosidad en la comisión de comportamientos lesivos de bienes jurídicos, lo cual fundamenta el desvalor o mayor desvalor social del injusto debido a las características criminógenas del ciberespacio como fuente de riesgos y, ii) en específico, para el caso del concurso entre comportamientos punibles pertenecientes a un mismo *iter criminis*, las TIC son un medio comisivo más que no siempre importarán un grado de desvalor suficiente como para independizar el injusto de preparación del injusto consumado.

En ese sentido, veremos supuestos donde el recurso a medios tecnológicos no suponga más que un “favorecimiento de la dinámica comisiva con la que se consigue el abuso [...]. En otros, el hecho tecnológico generará una lesividad de suficiente entidad como para poderla valorar con independencia de lo que pueda surgir o no después”³¹. Esta es la línea de pensamiento que considero debemos seguir.

²⁹ DE LA MATA, N. (2017). El contacto tecnológico con menores del art. 183 ter 1 CP como delito de lesión contra su correcto proceso de formación y desarrollo personal sexual. *Revista Electrónica de Ciencia Penal y Criminología*., pp. 23.

³⁰ SÁNCHEZ, M. (2023). Child grooming y concursos: evolución del tratamiento jurisprudencial en el ordenamiento jurídico español. *Política criminal*., pp. 428.

³¹ DE LA MATA, N. (2017). El contacto tecnológico con menores del art. 183 ter 1 CP como delito de lesión contra su correcto proceso de formación y desarrollo personal sexual. *Revista Electrónica de Ciencia Penal y Criminología*., pp. 24.

La existencia de importantísimos estudios científicos en el campo de la criminología demuestra efectivamente que las tecnologías de la información y la comunicación comportan una especial peligrosidad al facilitar la comisión de delitos. No debemos olvidar, sin embargo, que el derecho está conformado por hechos, valores y normas; y la dogmática penal no puede quedarse con el simple dato fáctico desprovisto de toda valoración. Esto cobra singular relevancia en los conflictos de delitos en el contexto de progresiones delictivas, donde habría que verificar si el comportamiento precedente ha obtenido en el caso concreto un desvalor lo suficientemente grave como para castigarlo autónomamente inclusive allí donde el delito fin se haya consumado, teniendo lugar un legítimo concurso de delitos. En sentido contrario, si el desvalor del uso de las TIC no ha sido lo suficientemente relevante, procederá un simple concurso de leyes. Es una cuestión que debe ser tratada finalmente caso por caso.

Las nuevas tecnologías son pues un dato fáctico más a valorar en este contexto, sus características brindan cierta protección al delincuente –anonimato, ausencia de vigilancia policial, facilidad de borrado de huellas, contacto con múltiples víctimas, etc.– que convierte su conducta antijurídica en un ataque sobre seguro, una especie de alevosía que constituye algunas veces una circunstancia agravante en los ordenamientos penales sustantivos. Así pues, a mi juicio, allí donde tal garantía de actuar desprovisto de riesgos se pierda, o sea muy mínima o irrelevante, por ejemplo, cuando la finalidad sexual se comete en el ámbito físico-presencial, los beneficios de las TIC también decaerán pues el delincuente se expone a una mayor probabilidad de ser descubierto o detenido, absorbiendo entonces el delito fin al acto preparatorio punible.

Lo que se quiere, por último, es que las penas sean proporcionales al desvalor del hecho, idea que subyace al principio del *non bis in idem* y al concurso de leyes y de delitos. Esto no nos debe llevar a la errónea conclusión de que la suficiente entidad del desvalor de las TIC deba probarse en cada tipo penal que requiera su uso como agravante³² o como elemento objetivo del tipo, puesto que en aquellos tal desvalor ya se presume como idóneo para fundamentar una pena o una agravación de la misma. Afirmar lo contrario sería desvirtuar el principio de legalidad.

³² Como sucede en el artículo 316-A del Código Penal peruano, que castiga con una pena agravada la apología al terrorismo a través de las tecnologías de la información y la comunicación.

Sin embargo, cabe traer a colación que la importancia que actualmente se le da al fenómeno de las nuevas tecnologías en la dogmática penal, tiene fecha de caducidad, pues tal como sostiene el profesor Agustina³³: “En unos años, todos los delitos se explicarán o se probarán con base en la suma de acciones y omisiones por medios físicos y virtuales. Las interacciones humanas serán completamente híbridas. En ese escenario, perdida la novedad del ciberdelito, carecerá de sentido referirse a una tipología distinta, tampoco desde el punto de vista de las estructuras de imputación”. Ello no le resta relevancia a la tarea dogmática que emprendemos algunos sobre el estudio de los llamados ciberdelitos, pues sigue siendo una cuestión de alta actualidad, una necesidad imperante, una transición hacia un nuevo mundo.

V. Conclusiones

El delito de *child grooming* es, al menos en el ámbito nacional, uno de los que menos atención ha recibido tanto a nivel doctrinal como jurisprudencial, lo que resulta preocupante teniendo en cuenta los desafíos que representa no solo por su cuestionada legitimidad en el ordenamiento penal sostenida por algunos autores debido a que se trata de un adelantamiento de las barreras de protección punitiva, sino también por los problemas concursales que plantea cuando la finalidad sexual pretendida por el *groomer* es conseguida.

A lo largo de este artículo hemos emprendido inicialmente un análisis de la tipicidad y naturaleza jurídica del grooming, bajo la interrogante de si el primer párrafo del artículo 5 de la Ley 30096 sanciona la lesión efectiva de la indemnidad sexual del menor o su mera puesta en riesgo. Al respecto hemos identificado tres posturas principales consistentes en las tesis del peligro abstracto, peligro concreto y de lesión. La peculiaridad de este tipo penal hace que comparta ciertas características con lo que suele entender la dogmática por peligro abstracto y concreto, no obstante, resulta patente que la doctrina mayoritaria, y también los pronunciamientos judiciales, conviene en reconocer la tesis del peligro en general (ya sea abstracto o concreto), no así con la tesis de lesión que adolece de un menor respaldo, lo que no significa que sus argumentos no sean atendibles.

³³ AGUSTINA, J. R. (2021). Nuevos retos dogmáticos ante la cibercriminalidad ¿Es necesaria una dogmática del ciberdelito ante un nuevo paradigma? *Estudios Penales y Criminológicos*, pp. 743.

Para la tesis de lesión, asumida por el autor, el ciberacoso lesiona ya la indemnidad sexual comprendida como el correcto y normal desarrollo de la sexualidad del menor, sin intromisiones dañosas, a efectos de garantizar eventualmente, una vez cumplidos catorce años, el buen y responsable ejercicio de su autodeterminación sexual. En este contexto, el grooming perturba y distorsiona ya la imagen que tiene el menor sobre su propia sexualidad al recibir propuestas libidinosas, habida cuenta de que la indemnidad del menor abarca tanto la esfera somática como la psicosexual. De cualquier forma, sea que se opte por una u otra postura, del análisis efectuado podemos llegar a un resultado concluyente, y es que el acoso online de menores constituye un adelantamiento de la protección penal, una especie de acto preparatorio donde se pretende evitar la comisión de otros delitos sexuales tradicionales.

Tal adelantamiento de las barreras punitivas tiene su legítimo fundamento en tres razones fundamentales: i) la multiplicidad de cursos lesivos que se pueden derivar del ciberacoso, como bien puede ser la consecución de las finalidades sexuales o la obtención de material pornográfico por parte del *groomer*, ii) la importancia del bien jurídico indemnidad sexual y iii) las características inherentes a las TIC □anonimato, facilidad para el borrado de huellas del delito, facilitación del contacto entre el victimario y múltiples víctimas potenciales, ausencia de guardianes capaces, etc. Las dos primeras razones dotan de un especial sentido delictivo al grooming, haciendo que el acto preparatorio pierda su equivocidad; la tercera, por otro lado, otorga un plus de desvalor al injusto por valerse de medios que vuelven a la conducta típica más gravosa y, en ese sentido, reprochable.

Por otro lado, cabe señalar que la regla general en materia concursal es que el inicio de la ejecución o la consumación del delito fin absorba el desvalor social del acto preparatorio, pues también hay una relación de subsidiariedad entre los grados de realización de un delito que justifica la aplicación del concurso de leyes en este caso. Esta subsidiariedad se pierde, sin embargo, cuando la conducta de preparación añade ciertos elementos que no prevé el delito fin y que, por ende, éste no abarcaría todo el desvalor de los hechos, procediendo así un concurso de delitos.

Ahora bien, el hecho de que entre el ciberacoso y los eventuales actos libidinosos o el acceso carnal haya un supuesto de progresión delictiva, no debe llevar a afirmar que siempre que la finalidad sexual pretendida por el *groomer* sea conseguida, tenga lugar un concurso de

leyes, toda vez que el medio comisivo tecnologías de la información y la comunicación, por lo general, agregan un plus de reprochabilidad al injusto. No obstante, no es menos cierto que muchas veces el uso de tales tecnologías solamente favorece la dinámica comisiva del grooming sin llegar a adquirir mayor relevancia. Por ende, solamente cuando el grooming en el caso concreto adquiriera una lesividad suficiente como para merecer su punición autónoma, cabrá un concurso de delitos, caso contrario, se deberá proceder con el concurso de leyes.

Consideraciones éticas en la implementación de sistemas de inteligencia artificial para la selección y contratación de personal

Juan Miguel De los Santos Esteve*

Resumen.- En el presente artículo abordaremos sobre la incidencia de la ética en el uso y desarrollo de los sistemas de inteligencia artificial utilizados para gestionar procesos de selección de personal. Para lo cual, analizaremos el concepto de inteligencia artificial, así como el de ética y trataremos acerca de las recientes leyes que establecen obligaciones jurídicas de su uso para contratar o seleccionar trabajadores.

Palabras clave.- Inteligencia Artificial – Principios éticos – Proceso de Selección – Prevención de Riesgos. – No discriminación

Abstract.- In this article, we will examine the impact of ethics on the use and development of artificial intelligence systems employed in personnel selection processes. To that end, we will analyze the concept of artificial intelligence, as well as that of ethics, and discuss recent laws that establish legal obligations for its use in hiring or selecting workers.

Keywords.- Artificial Intelligence – Ethical Principles – Selection Process – Risk Prevention – Non-discrimination

* Analista legal en el Ministerio de Trabajo y Promoción del Empleo.

** Agradezco al profesor Juan Gorelli Hernández, por su recomendación en la elección y desarrollo de la temática abordada. Abogado por la Pontificia Universidad Católica del Perú.

*Cada vez que las sociedades atraviesan
por períodos críticos en sus aparatos productivos,
el tema de la Ética sale a relucir.*

– Antonio Romero, 1998¹

I. Consideraciones preliminares sobre la ética y su relación en el ámbito del derecho del trabajo.

Se define la ética como “(...) el conjunto de ideas, principios e ideales que una sociedad imagina para sí misma, con el objetivo de afirmar el bien y negar el mal. Así, la Ética trata de relaciones humanas: de qué hace la gente con otra gente. Regula la conducta entre nosotros”² (Barilko, 1998). Por tanto, como subcampo de la filosofía, la ética determina el conjunto de valores, principios e ideales como el respeto, la integridad o la justicia que rigen una sociedad, a efectos encaminarla hacia un referente o modelo deseado, como la utopía.

En base a estos principios y valores, se busca entonces orientar y prever la conducta moral del ser humano como parte de una sociedad, es decir, lo que hace una persona frente a su homólogo, diferenciando entre lo que significa el accionar de un buen y un mal comportamiento, un comportamiento coherente e incoherente con el respeto hacia los demás: “En general, la ética es una disciplina filosófica, que tiene un carácter normativo y práctico, sobre cómo actuar en el entorno social, donde se inserta el individuo, aplica los principios éticos para conciliar la moral, los deseos y las capacidades de las personas para actuar de manera coherente” (González & Martínez, 2020)³. Así pues, la ética busca armonizar la libertad inherente del ser humano para actuar según sus deseos y aspiraciones con el deber de que este accionar sea moral, y se prevea las posibles consecuencias de sus actos, evitando hacer daño

¹ ROMERO, A. (1998). La ética del trabajo: un caso particular en Barquisimeto. Como se cita en ERMIDA, O. (2005). Ética y derecho del trabajo. IUS ET VERITAS, 15(30), pp. 228-246.

² BARYLKO, J. (1998). Ética para argentinos. Buenos Aires, Argentina: Editorial Aguilar.

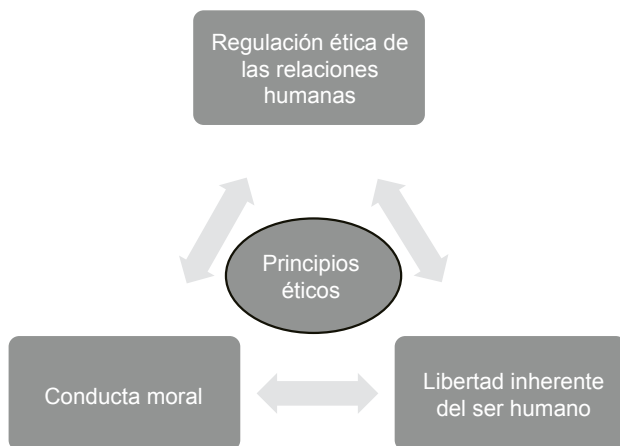
³ GONZÁLEZ, M. & MARTÍNEZ, D. (2020). Dilemas Éticos en el Escenario de la Inteligencia Artificial. Economía & Sociedad, 25(57), pp. 1-17.

y procurando el respeto hacia a sus similares como parte del mismo conjunto social (Cuadro N° 01).

Ahora, en el marco de un Estado Constitucional de Derecho, muchos de estos valores y principios son respaldados por el mismo Estado y las constituirán como fundamentos de conducta que regirán el comportamiento de las personas. Así, estas normas jurídicas - principios establecen pautas generales que irradian sobre las ramas que componen nuestro ordenamiento jurídico, como por ejemplo, la del derecho laboral.

Así pues, en pro del desarrollo social, la ética busca regular nuestra conducta determinando un conjunto de valores y principios, conciliando nuestra libertad para actuar conforme a nuestra voluntad con el deber de que este accionar sea moral, conforme a tal conjunto de valores, y, en consecuencia, se evite hacer daño a nuestros similares, como parte de un mismo conjunto social.

Cuadro N° 01



Dicha finalidad no se exceptúa en el marco de una relación laboral, en el que existe un marco asimétrico entre las dos personas que constituyen tal relación jurídica. Así, si bien esta relación la puede constituir, en principio, dos personas similares entre sí, jurídicamente una ostenta más poder y, por tanto, más libertad de acción frente a su similar, consecuencia de la capacidad de tomar decisiones que puedan afectar (de manera positiva o negativa) la situación jurídica de su contraparte,

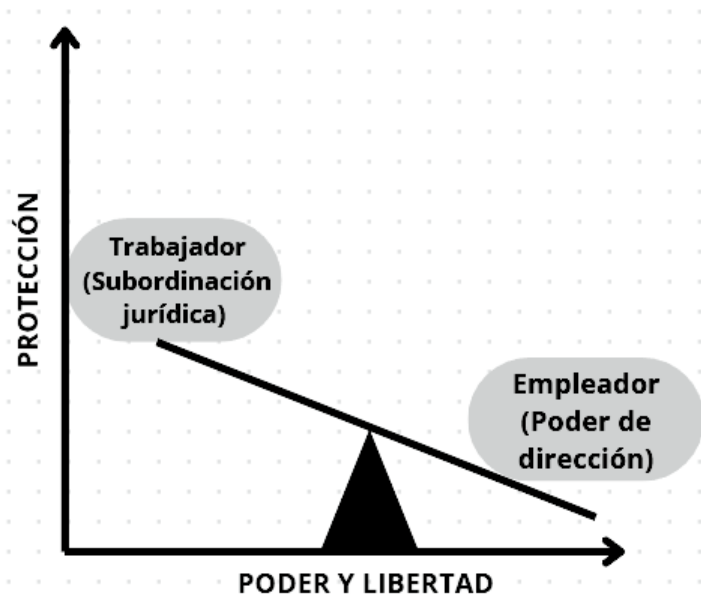
quien consecuentemente, y solo en el marco de esta relación laboral, sufrirá inevitablemente una disminución de su libertad.

Aunque parezca injusto, tratándose de dos homólogos entre sí, lo cierto es que en una relación laboral este marco asimétrico entre ambas partes es vital. Así pues, la complejidad de nuestro conjunto social se refleja en que, por un lado, seamos bastante similares entre sí, pero también en que diferimos en muchos otros aspectos, como nuestra manera de pensar y, en consecuencia, las diferentes decisiones que tomaríamos en una situación similar. Ante ello, surge la necesidad del establecimiento de jerarquías, de una o algunas personas a la que se les atribuyan más poder y capacidad de decisión, para que se coordinen esfuerzos hacia un interés unitario. En el marco de una relación laboral, dicha coordinación de esfuerzos deberá realizarse a través del poder de dirección, por medio del cual, el empleador puede organizar y reglamentar la manera en que los trabajadores deben actuar y disponer sus esfuerzos en el centro de labores, así como supervisar y, de ser el caso, sancionar alguna conducta.

Por tanto, en el marco de una relación jurídica en el que la distribución desigual de poder conlleva a un marco asimétrico entre dos similares que la constituyen, la regulación de la conducta en base a un conjunto de valores y principios en la que se prevé que nuestro accionar sea moral cobra especial importancia, pues un accionar inmoral podría conllevar a un abuso de poder. De este modo, la ética cobra un papel más relevante dentro de una relación laboral, en la que su impacto es más fuerte y necesario —a comparación de otras relaciones jurídicas simétricas— ante riesgos de abusos de una parte que necesariamente debe ostentar más poder.

Así pues, si bien la ética toma un papel más relevante en estas situaciones, lo cierto es que, ante la necesidad de la existencia de una asimetría entre las partes de la relación laboral, se procurará una atenuación de tal asimetría sin que se busque una igualdad entre las partes, perviviendo una parte fuerte y otra débil. En consecuencia, la regulación de la conducta de las partes en base a un conjunto de valores en la que se prevea el respeto y se evite hacer daño se traducirá en una finalidad protectora que amparará a la parte más débil del contrato (Cuadro N° 02).

Cuadro N° 02



En base a esto, se manifiesta el importante contenido ético en el derecho laboral, el cual asume un rol protector de la parte que se mantendrá con menos poder en la relación laboral: “El objetivo axiológico del Derecho del Trabajo y de la Seguridad Social es claramente, la protección del débil en la relación de trabajo, la promoción de la igualdad, la búsqueda de la paz social y de la justicia social, la promoción de la autonomía colectiva” (Ermida, 2005)⁴.

Por tanto, una relación jurídica de naturaleza laboral se regula de manera diferente a comparación de relaciones jurídicas de otro tipo, debido a la asimetría inherente entre las partes que constituyen tal relación. La atenuación de la desigualdad entre las partes, la protección de la parte

⁴ ERMIDA, O. (2005). Ética y derecho del trabajo. IUS ET VERITAS, 15(30), 228-246, pp. 232.

más débil del contrato laboral, entre otros aspectos, promueven valores morales como la igualdad, la justicia y la paz social que debería regir nuestra sociedad enmarcada en un Estado Constitucional de Derecho.

Por tanto, la ética cobra una especial importancia en el marco de una relación laboral ante su naturaleza asimétrica, y el riesgo de que se constituya un abuso de poder, aunado también a que un contrato laboral es uno de tracto sucesivo, es decir, que no se agota ni culmina con la realización de una tarea. Junto a lo anterior, Ermida (2005) además resalta lo siguiente:

Si observamos conjuntamente la (...) implicación personal del trabajador en la ejecución de la relación de trabajo y la continuidad o durabilidad de las relaciones de trabajo, apreciaremos la especial importancia del contenido ético de la relación de trabajo, que es diferente al contenido ético de un contrato de ejecución instantánea⁵.

Por tanto, al ser el contrato laboral uno de tracto sucesivo prolongado en el tiempo en el que se vinculará en gran medida la vida, el tiempo y la salud de la persona del trabajador, es crucial conciliar la libertad inherente del ser humano para actuar según sus deseos con el deber de que este accionar sea moral, es decir, que en el ámbito del derecho laboral constituiría en la exigencia de condiciones mínimas protectoras para el trabajador frente a la libertad contractual que podrían tener las partes en una relación jurídica de distinta naturaleza.

Así, surge un reconocimiento de derechos específicos e inespecíficos que protegen al trabajador, quien, al invertir gran parte de su tiempo y salud en esta prestación de carácter personal y prolongada en el tiempo, otorga una significativa dimensión humana al trabajo prestado, de ahí que la Declaración de Filadelfia comience resaltando, en su inciso a) artículo I, como primer principio fundamental que el trabajo no es una mercancía⁶. Dado que, considerándolo como un bien o mercancía que puede sustituirse o descartarse sin más, se desligaría el factor humano del trabajo y los derechos que goza el trabajador, se desnaturalizaría la

⁵ *Ibid.*, pp. 235.

⁶ Organización Internacional del Trabajo. (1944). Declaración relativa a los fines y objetivos de la Organización Internacional del Trabajo (Declaración de Filadelfia) <https://webapps.ilo.org/static/spanish/inworkcbpolicyguide/declaraciondefiladelfia1944.pdf>

relación jurídica generada entre las partes, suprimiendo el contenido ético del derecho laboral ante la no necesidad ya de proteger ni atenuar una desigualdad existente si es que el trabajo se reduce solo a la venta y compra de una mercancía. Así pues, dicho factor humano proviene del valor intrínseco y la dignidad que tiene toda persona por su misma condición de tal que la hace merecedora del disfrute de determinados derechos durante e incluso previamente al inicio de una relación laboral, independientemente del mecanismo o tecnología que se use para gestionar los procesos organizacionales de un centro de labores.

II. La implementación de la ética en los sistemas de la inteligencia artificial

La inteligencia artificial (en adelante, la “IA”) es una tecnología cuya evolución se ha dado rápidamente generando muchas ventajas, como la reducción de costos o de tiempo en el procesamiento de cantidades significativas de datos. Sin embargo, su evolución no debe estar encaminada solo en cuanto al incremento de su eficiencia, sino también en cuanto a la moral y la ética. Así, toda aplicación de la ciencia y la tecnología debe partir del respeto y la protección a las personas, evitando hacerles daño, reduciendo los perjuicios y maximizando sus beneficios.

Por tanto, la ética influye en nuestra forma de utilizar la tecnología y, por tanto, a los sistemas de IA, previendo de que nuestro comportamiento sea acorde a los valores morales que una sociedad reconoce como parte de sí, dando lugar a lo que se denomina como la “ética de la IA”:

(...) iv) La ética aplicada, a la que le preocupa lo que estamos obligados a hacer (o lo que se nos permite hacer) en una situación específica (...) La ética de la inteligencia artificial se considera generalmente un ejemplo de la ética aplicada que se centra en los problemas normativos que plantea el desarrollo, despliegue y utilización de la IA⁷.

De este modo, aun cuando parezca que los efectos positivos o negativos provengan directamente de la tecnología y de computadoras con inteligencia asimilable a la humana, no olvidemos que el propósito que le asignemos y nuestro comportamiento en torno a la IA pueden y deben ser

⁷ Comisión Europea, Dirección General de Redes de Comunicación, Contenido y Tecnologías. (2019). Directrices éticas para una IA fiable. Oficina de Publicaciones. <https://data.europa.eu/doi/10.2759/14078>

encausados bajo principios éticos, pues «(...) las características positivas y negativas inherentes a los seres humanos se reflejan en los resultados de la revolución científica derivada de los avances de la informática. Se trata de decisiones morales en el entorno digital de las personas, sobre cómo las emplean y la forma en que se relacionan entre sí»⁸ (Ramos, 2018, como se citó en González & Martínez, 2020).

Un dispositivo o aparato electrónico con tecnología de IA no puede evaluar si el procesamiento de ciertos datos y la decisión o la solución a la que llegue pueda generar efectos negativos indirectos hacia un determinado sector de la sociedad, pues se limita a seguir secuencialmente las instrucciones instaladas en su algoritmo creado especialmente para generar la mayor precisión y eficacia en la decisión, predicción o solución que proponga. Así pues, una computadora carece de sentido moral o preocupación sobre lo que se considera correcto o incorrecto. Ante esta situación, la ética de la IA establece pautas de comportamiento de las personas en torno al desarrollo, programación y uso de sistemas de IA, de manera que se prevea que tales conductas no generen daño a la sociedad y se continúe aprovechando de los beneficios que genera promoviendo su utilización. De hecho, las cuestiones éticas que implican el uso de la IA significan una limitación para su implementación en la gestión de estructuras organizativas empresariales, pues las principales barreras que impiden ello incluyen habilidades y experiencia limitadas en IA (33%), demasiada complejidad de datos (25%) y preocupaciones éticas (23%)⁹.

Por lo tanto, la ética de la IA armoniza el deber de un comportamiento responsable durante todo el ciclo de vida de la IA y el aprovechamiento de sus beneficios, promoviendo el desarrollo y uso de una IA eficaz y confiable. Ante tal objetivo, son principalmente la Comisión Europea (en adelante, “CE”) a través del documento “Directrices Éticas para Una

⁸ RAMOS, M. (2018). La ética digital se consolida como un aspecto clave en la toma de decisiones. CIO. Como se cita en GONZÁLEZ, M. & MARTÍNEZ, D. (2020). Dilemas Éticos en el Escenario de la Inteligencia Artificial. Economía & Sociedad, 25(57), pp. 1-17.

⁹ IBM. (2024). Data suggests growth in enterprise adoption of AI is due to widespread deployment by early adopters. IBM Newsroom. <https://newsroom.ibm.com/2024-01-10-Data-Suggests-Growth-in-Enterprise-Adoption-of-AI-is-Due-to-Widespread-Deployment-by-Early-Adopters>

IA fiable” y la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura – UNESCO, a través del documento “Recomendación sobre la ética de la inteligencia artificial” las que han emitido pautas o recomendaciones estructuradas en una lista de principios éticos en el uso y desarrollo de la IA, que se inspiran en valores morales como la libertad, democracia, justicia y paz social.

Por tanto, a continuación, analizaremos las implicancias éticas en el uso de la IA para la selección de personal en empresas o entidades públicas, haciendo referencia a las directrices o principios más relevantes de ambos documentos para encausar un uso coherente de la misma en este campo de acción:

- a. Principio de autonomía humana: se prevé que el desarrollo de sistemas de IA se encuentre centrado en las personas, quienes deben controlar y supervisar su funcionamiento. En materia de selección de personal, la decisión final y elección del candidato ideal debería estar respaldada por una supervisión humana y no realizarse de manera automática por el sistema de IA.
- b. Principio de responsabilidad: dado que existe supervisión humana sobre las decisiones que tome la IA, también debe existir una responsabilidad atribuible a una persona física o jurídica por los resultados de dichas decisiones. Por ejemplo, podría responsabilizarse a al ingeniero que desarrolló un algoritmo que favorece a personas de una determinada condición económica en el marco de un proceso de selección.
- c. Principio de transparencia y explicabilidad: para que una persona pueda identificar realmente si es que alguno de sus derechos ha sido vulnerado, debería saber primero, explicado de manera sencilla, en que se basó la IA para realizar una determinada decisión. De este modo, un postulante debería saber, primero, si es que un proceso de selección será gestionado parcial o totalmente por una IA y, segundo, conocer de forma sencilla los motivos de la decisión final.
- d. Principio de prevención de riesgos: el uso de la IA no debe provocar daños a las personas, por lo que se prevé una evaluación de riesgos previa a su funcionamiento. Así, siendo que no todo uso de IA genera los mismos beneficios o los mismos riesgos o repercusiones en la sociedad, deberá ponerse especial atención a los mecanismos que puedan afectar de manera directa o indirecta a los seres humanos, sobre todo, si se realiza en un marco de

asimetría entre personas, como podría ser el caso de que se use para la selección de personal, en la que los derechos a la privacidad y no discriminación de los postulantes podrían verse afectados: « Prestar una atención especial a (...) colectivos que se hayan visto históricamente desfavorecidos o que se encuentren en riesgo de exclusión o en situaciones caracterizadas por asimetrías de poder o de información, como las que pueden producirse entre empresarios y trabajadores o entre empresas y consumidores¹⁰.

i. Directrices éticas en el marco de un proceso de selección gestionado por IA respecto al riesgo contra la privacidad de los postulantes

Como mencionamos previamente, la IA de aprendizaje automático ha experimentado un rápido crecimiento, maximizando sus beneficios en cuanto al procesamiento de datos de diversas fuentes, lo que hace que la tecnología se perfeccione, aprenda y pueda ofrecer cada vez decisiones más precisas. Esto debido sobre todo al Big Data (en adelante, “BD”) que se define como grandes cantidades de datos y conjuntos de datos complejos que pueden ser estructurados (nombres o direcciones de clientes), no estructurados (archivos de audio o publicaciones en redes sociales) o semi-estructurados (archivos JavaScript o XML) (Mucci & Stryker, 2024)¹¹. Así pues, siendo que los datos son el elemento vital en el funcionamiento de la IA, una enorme cantidad de estos significa un mayor aprendizaje, aunque no siempre sea el más óptimo.

Debido a la digitalización, muchos de nuestros datos son rápida y fácilmente accesibles a través de cualquier dispositivo con acceso a internet, como, por ejemplo, saber de cuántos inmuebles una persona es propietaria o de opiniones pasadas de toda índole publicadas en redes sociales de acceso público.

De modo tal, que el BD puede suministrar a los sistemas de IA datos de toda clase y materia para que esta pueda encontrar en cuestión de segundos patrones o correlaciones entre estas y aprender a partir de esta nueva información autogenerada.

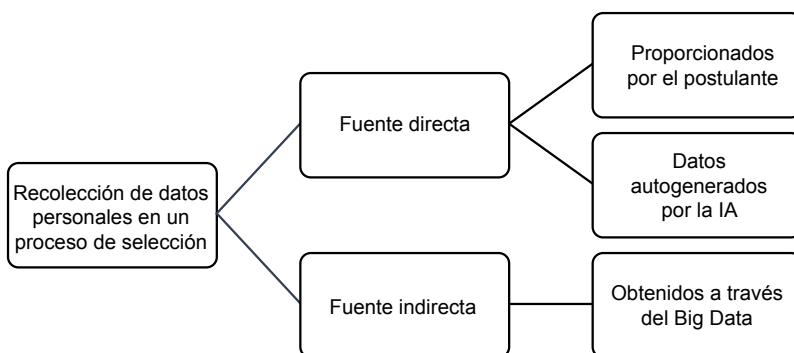
¹⁰ Comisión Europea, Dirección General de Redes de Comunicación, Contenido y Tecnologías. (2019). Directrices éticas para una IA fiable. Oficina de Publicaciones.

¹¹ MUCCI, T. & STRYKER, C. (2024). What is big data analytics? Recuperado de: <https://www.ibm.com/topics/big-data-analytics>

Así pues, si bien la propia naturaleza del contrato laboral, como de tracto sucesivo y prestación personalísima, incide en la importancia de su etapa previa (proceso de selección), de quién será contratado de manera indefinida una vez superado el periodo de prueba, es también su propia naturaleza la que abarca un importante componente ético y el respeto de los derechos fundamentales del trabajador y de la persona que postula a una determinada convocatoria.

En el marco de una convocatoria gestionada por IA, los datos personales a los que puede acceder esta tecnología pueden ser recabados bien de una fuente directa, como las facilitadas por el postulante al registrarse en una determinada plataforma virtual (como su número de DNI o fecha de nacimiento) o también generada por la misma IA, cuya habilidad de aprendizaje y reconocimiento de patrones puede inferir nueva información a partir de los datos facilitados por el postulante; o bien pueden ser recabados de una fuente indirecta o ajena, la cual sería la que fue accesible a través del BD, como podría ser artículos jurídicos que elaboraste y publicaste anteriormente en una página web, noticias de prensa divulgadas que aluden a tu persona o saber tu puesto en el cuadro de méritos de una convocatoria pública pasada en la que participaste (Cuadro N° 3).

Cuadro N° 03



Todos esos datos podrían ser procesados a través del algoritmo de la IA, en la que se identificarán entre rasgos favorables o desfavorables para predecir finalmente quién podría adaptarse más rápido a la empresa y

tener el mejor desempeño laboral. Sin embargo, debido a que muchas veces la decisión final trasciende de la información ofrecida directamente, pudiendo accederse a data personal o hasta sensible, se presenta el riesgo que pueda estarse vulnerando la privacidad de algún postulante. Ante dicho tipo de riesgos, la CE y la UNESCO establecen pautas éticas del uso de la IA:

- a. Intimidad y protección de datos: la privacidad de las personas debe ser respetada a lo largo de todo el ciclo de vida de los sistemas de IA, debiendo recopilarse, inferirse o compartirse datos de forma coherente. Es decir, en el marco de un proceso de selección, deberá preverse utilizar solo los datos necesarios para identificar al candidato ideal, entre los que pueden considerarse datos personales o no personales, siendo en todo caso prohibido el análisis de datos sensibles de la persona, a los que la IA podría acceder o inferir a través de data suministrada por el BD, como por ejemplo, la inferencia de la orientación sexual de un postulante a partir de los perfiles a los que da “follow” o publicaciones que da “like” en redes sociales. Asimismo, en caso de que una empresa decida compartir los resultados de un test de personalidad con una empresa especializada en reclutamiento para una opinión complementaria, deberá hacerlo garantizando la confidencialidad de los datos personales.
- b. Seguridad y protección: en este caso, los datos recolectados y posteriormente almacenados por el usuario deben resguardarse para prevenir riesgos de seguridad o protección de la información, como filtraciones de datos. Por ejemplo, si una empresa decide almacenar la información de ciertos postulantes prospectos para invitarlos a convocatorias futuras, este archivo debe realizarse garantizando la integridad y protección de los datos, generándose una obligación de protección a la privacidad que persiste incluso después de culminado el proceso de selección.

En resumen, a través de estos dos principios éticos en particular, se pretende encausar el uso que pueda darse a herramientas como la IA para evitar en la medida de lo posible riesgos relacionados a la afectación al derecho de la privacidad de las personas y, en el marco de un proceso de selección, el de los postulantes. Y es que, ante la intención de una decisión o predicción más precisa, se procura dotar a la IA de la mayor cantidad de datos posible, entre los cuales podrían extraerse y

analizarse, voluntaria o involuntariamente, datos personales (sensibles o no sensibles) sin el consentimiento previo debido. Finalmente, la función de la IA será evaluar como favorable o desfavorable determinados rasgos identificados a partir de los datos proporcionados sobre los participantes de un proceso de reclutamiento, pudiendo generarse un trato discriminatorio.

ii. Directrices éticas en el marco de un proceso de selección gestionado por IA respecto al riesgo de tratamiento discriminatorio hacia los postulantes

Anteriormente se creía que, tratándose de algoritmos matemáticos que tomaban decisiones, lo lógico sería que una ventaja que aportaría la IA sería la desaparición de sesgos y subjetividades que muchas veces influían en las decisiones humanas. Sin embargo, es todo lo contrario: “La discriminación algorítmica, no obstante, añade nuevas dimensiones al problema de la discriminación y es que los sistemas de IA no solo reproducen las discriminaciones existentes, sino que las sistematizan y las amplifican a grande escala y a una velocidad vertiginosa” (Bolukbasi et al, 2016)¹². Es decir, en caso de que una empresa lleve años usando una IA que, mediante su proceso de aprendizaje en base a su experiencia, asimiló que es favorable que los postulantes mayores a 45 años sean descartados automáticamente de cualquier proceso de selección convocado por la empresa, el *modus operandi* de la IA generará inflexibilidad y automatización en el uso de tal fundamento de decisión y, a diferencia de las decisiones humanas que tienden a variar con el paso del tiempo, la automatización de la IA generará constancia y repetición en cuanto a dicho trato discriminatorio, reduciendo completamente las posibilidades de una persona mayor a tal edad de acceder a algún empleo en tal centro de labores: “Schellmann cree que el mayor riesgo que plantea este tipo de software para los puestos de trabajo no es que las

¹² BOLUKBASI, T., CHANG, K., ZOU, J., SALIGRAMA, V., & KALAI, A. (2016). Man is to Computer Programmer as Woman is to Homemaker? Debiasing Word Embeddings. Proceedings of the 30th International Conference on Neural Information Processing Systems, NIPS'16. Como se cita en Ginés, A. (2024). Algoritmos sesgados en el trabajo. Consideraciones entorno a su tratamiento jurídico. Trabajo y derecho: nueva revista de actualidad y relaciones laborales, (19), pp. 1-37.

máquinas ocupen los puestos de los trabajadores, como suele temerse, sino que les impidan conseguir un puesto” (Lytton, 2024)¹³.

El trato discriminatorio producido por IA, que podría darse también en el marco de una convocatoria laboral, puede producirse a lo largo de todo su ciclo de todo su ciclo de funcionamiento (Cuadro N° 04).

Cuadro N° 04



A. Desarrollo discriminatorio de la IA

La discriminación puede provenir desde la etapa en la que algún ingeniero especializado en software desarrolló el algoritmo de una IA simbólica o de aprendizaje automático, durante la cual puede haber agregado de manera voluntaria que determinadas características o rasgos de la persona, como su raza o condición económica, representen puntos en contra o desfavorables en el marco de un proceso de selección.

Aunque también este desarrollo discriminatorio podría darse de manera involuntaria, pues dado que la IA es desarrollada por un

¹³ LYTTON, C. (2024). AI hiring tools may be filtering out the best job applicants. BBC Worklife. <https://www.bbc.com/worklife/article/20240214-ai-recruiting-hiring-software-bias-discrimination>

ser humano, su pensamiento o sesgos positivos y negativos podrían influenciar inconscientemente en su desarrollo, lo que generaría posteriormente que la IA considere también determinados rasgos como favorables o desfavorables, positivos o negativos en una persona.

Un ejemplo sobre este tipo de discriminación se presentó en agosto de 2023, cuando la Comisión para la Igualdad de Oportunidades en el Empleo (EEOC, por sus siglas en inglés) demandó a tres empresas que brindaban servicios de tutoría bajo la marca “iTutorGroup”, sobre la base de que esta violaba la Ley de Discriminación por Edad en el Empleo de 1967, pues el programa de contratación de IA que utilizaba rechazaba automáticamente a las candidatas mujeres de 55 años o más y a los candidatos varones de 60 años o más. Finalmente, iTutorGroup acordaría una indemnización a favor de los postulantes rechazados automáticamente (Kempe, 2024)¹⁴.

B. Entrenamiento discriminatorio de la IA

A diferencia del anterior supuesto, este tipo de discriminación abarca la etapa post-desarrollo de la IA, por lo que solo puede ser realizada por una IA de aprendizaje automático: «(...) cuando esos datos sobrerrepresentan o sobrerepresentan a ciertos grupos, pueden producirse resultados sesgados. (...) Esto podría provocar que la herramienta rechace a candidatos calificados que poseen las habilidades necesarias pero cuyos currículos no fueron comprendidos con precisión por la herramienta»¹⁵.

Un caso ilustrativo sobre esto se dio cuando los programadores de la empresa “Amazon” suministraron a la IA (que funcionaba como herramienta de filtro y selección de CVs) con solo datos contenidos en currículums de hombres, dado que estos representaban en su mayoría a quienes trabajaban en tal empresa. Debido a esto, la IA

¹⁴ KEMPE, L. (2024). Navigating the AI employment bias maze. American Bar Association. https://www.americanbar.org/groups/business_law/resources/business-law-today/2024-april/navigating-ai-employment-bias-maze/

¹⁵ *Ídem*.

dio preferencia a los CVs de hombres, dejando en desventaja a las mujeres postulantes (Ayoub, 2022)¹⁶.

C. Autoaprendizaje discriminatorio de la IA

Finalmente, y una vez ya entrenada una IA usada como herramienta de selección de personal, la cual aprende automáticamente a partir de su experiencia de uso, esta aprenderá y generará su propia información para dar como resultado predicciones cada vez más precisas. Cabe resaltar que, como señalamos anteriormente, la IA es amoral y se basa principalmente en mejorar su eficiencia, más allá de que pueda producir daños a un sector de la sociedad, por lo que un trato discriminatorio sería considerado justificado por esta siempre que le permita brindar cada vez mejores predicciones en favor de los intereses de quienes la implementan.

Un ejemplo ilustrativo sobre este tipo de discriminación es el de la *start-up* “Gild”, la cual ofrecía servicios de búsqueda de talento a empresas. El modelo encontró una correlación estadística entre las habilidades de codificar de una persona, su participación en foros de programación y la visita de páginas web de manga japonés, actividades que eran practicadas en casi su totalidad por hombres. En este caso, el algoritmo identificó una correlación estadística entre visitar una página de manga japonés y buenas habilidades para codificar y, en consecuencia, lo reproducía en sus decisiones, generando indirectamente una desventaja sobre las mujeres postulantes¹⁷ (Ginés, 2024). Cabe resaltar que en cada uno de los tipos de discriminación antes señalados puede identificarse tanto discriminación del tipo directa e indirecta. Así pues, discriminación directa sería por ejemplo el caso de “iTutorGroup”, en el que la IA se basaba directamente en la edad y el sexo de los postulantes para filtrar automáticamente sus CVs

¹⁶ AYOUB, S. (2022). Recruitment by robot: how AI is changing the way Australians get jobs. The Guardian. <https://www.theguardian.com/technology/2023/oct/23/ai-recruitment-job-search-artificial-intelligence-employment>

¹⁷ GINÉS, A. (2024). Algoritmos sesgados en el trabajo. Consideraciones entorno a su tratamiento jurídico. Trabajo y derecho: nueva revista de actualidad y relaciones laborales, (19), pp. 1-37.

y descartarlos. Por otro lado, un ejemplo de trato discriminatorio generado involuntaria e indirectamente sería el del caso “Gild”.

En ese sentido, se han establecido directrices éticas con la finalidad de evitar este tipo de riesgos sobre las personas, especialmente en el marco de una relación jurídica laboral:

- a) Principio de equidad y no discriminación: mediante el uso de la IA, se busca evitar que se reproduzcan, sistematicen y magnifiquen tratos discriminatorios o sesgos injustos: “Los actores de la IA deberían hacer todo lo razonablemente posible por reducir al mínimo y evitar reforzar o perpetuar aplicaciones y resultados discriminatorios o sesgados a lo largo del ciclo de vida de los sistemas de IA, a fin de garantizar la equidad de dichos sistemas”¹⁸.

De este modo, si bien estas directrices éticas son un buen punto de partida para encausar el comportamiento humano en el uso de la IA como herramienta de selección de personal, propiamente no pueden asegurar el comportamiento ético en torno a la IA de los actores involucrados en su ciclo de vida, motivo por el cual recientemente se vienen estableciendo medidas jurídicas que, inspirados en dichos principios, regulan o regularán a futuro el uso que debería darse a dicha tecnología.

III. Medidas jurídicas sobre la regulación del uso y desarrollo de la IA como herramienta para seleccionar personal

Del análisis elaborado por el Dr. Gutiérrez en el “Documento de Consulta sobre la Regulación de la Inteligencia Artificial” (*Consultation Paper On AI Regulation*) se identifica que las leyes y proyectos de ley publicados o propuestos durante estos últimos años, siguen nueve enfoques regulatorios complementarios entre sí (ordenados desde el menos al más intervencionista) como los basados en principios éticos, en potenciales riesgos del uso de la IA, en el acceso a la información y transparencia, entre otros¹⁹ (Gutiérrez, 2024). Así es como la mayoría de

¹⁸ UNESCO. (2022). Recomendación sobre la ética de la inteligencia artificial. https://unesdoc.unesco.org/ark:/48223/pf0000381137_spa

¹⁹ GUTIÉRREZ, J. (2024). Consultation paper on AI regulation: emerging approaches across the world. UNESCO. <https://unesdoc.unesco.org/ark:/48223/pf0000390979>

las leyes y propuestas de regulación sobre la materia abarcan más de uno de estos enfoques y plasman su regulación a través de normas legales o reglamentarias.

Como, por ejemplo, el 5 de julio de 2023, en el Perú se publicó la Ley 31814, “Ley que promueve el uso de la IA en favor del desarrollo económico y social del país” (en adelante, la “Ley”) y, posteriormente, se presentó el Proyecto de Reglamento de la Ley 31814 (en adelante, el “Proyecto de Reglamento”), en el que se complementan más enfoques regulatorios. De este modo, la Ley comienza estableciendo una lista de principios éticos en el uso y desarrollo de la IA, verificándose inicialmente el enfoque basado en principios éticos.

Junto con el caso peruano, son muchas otros proyectos de ley que abordan el enfoque “Basado en principios éticos” como punto de partida, como el Proyecto de Ley 059 / 2023 – Senado de Colombia, “Establecimiento lineamientos de política pública para el desarrollo, uso e implementación de la inteligencia artificial”, o el publicado por la Cámara de Diputados de Chile, “Proyecto de ley que regula los sistemas de inteligencia artificial, la robótica y las tecnologías conexas en sus distintos ámbitos de aplicación.”

Luego, basado en el enfoque basado en potenciales riesgos del uso de la IA, si bien las legislaciones a nivel global clasifican de manera parecida los niveles de riesgo de uso de la IA, como por ejemplo, mediante el artículo 14 del Proyecto de Reglamento, la legislación peruana lo hace en cuanto a implementación de IA de riesgo bajo, medio, alto e inaceptable; por otro lado, la legislación canadiense, a través del Apéndice B - Niveles de evaluación de impacto de la “Directiva sobre la toma de decisiones automatizadas” (*Directive on Automated Decision-Making*) lo hace en cuanto a la reversibilidad y la prolongación del daño que podría generar el uso de la IA, clasificándolo en decisiones de nivel I, II, III y IV. No obstante, tanto en las leyes o proyectos de ley a nivel global, como la brasilera (inciso III del artículo 17 del Proyecto de Ley 2338, “Dispõe sobre o uso da Inteligência Artificial”), chilena (inciso 4 del artículo 4 de su proyecto de ley), europea (anexo III del Reglamento 2024/1689 “Reglamento de Inteligencia Artificial”) y peruana (inciso 2 del artículo 14 del Proyecto de Reglamento) coinciden en establecer como una IA de alto riesgo la utilizada en el marco de la contratación y selección de personal.

Así pues, como señalamos anteriormente, en el marco del uso de sistemas de IA, se pone especial énfasis a aquellos que pueden afectar

directa o indirectamente a las personas, sobre todo si se trata de marcos asimétricos de poder, como la relación laboral entre empleador y trabajador. Ante ello, el derecho laboral plantea la atenuación (mas no eliminación) de tal asimetría de poder y amparar al trabajador estableciendo condiciones protectoras para sus derechos específicos e inespecíficos. Por consiguiente, el uso de la IA en el marco de una relación laboral, la cual inevitablemente genera un incremento de la asimetría entre las partes, se debe establecer un nivel de protección más elevado estableciendo condiciones o requisitos específicos adicionales a los anteriormente señalados para su uso de todo sistema IA en general.

Asimismo, específicamente en cuanto al uso de la IA para la selección de personal, como señalamos líneas anteriores, esta representa un considerable riesgo a los derechos fundamentales del trabajador, principalmente en cuanto a sus derechos a la privacidad y no discriminación. Y es que la facilidad de acceso directo o indirecto y procesamiento de data personal o sensible del trabajador, así como la posibilidad de reproducir y magnificar a gran escala sesgos o tratos discriminatorios que la mayoría de las veces son de difícil identificación, pueden afectar las perspectivas laborales y proyecto de vida de la persona, perpetuando la negativa de su acceso a un empleo que muchas veces es el principal medio de subsistencia propia y familiar. Por tanto, en la legislación comparada, se establecen listados de las obligaciones específicas para los sistemas basados en IA para el uso de selección y contratación de personal, y para todo sistema considerado de alto riesgo.

Por ejemplo, en la legislación brasileña, conforme al principio de prevención de riesgos, el inciso II del artículo 20 del Proyecto de Ley 2338, instituye el uso de herramientas de registro automático de la operación del sistema de IA, para permitir su evaluación e identificar potenciales sesgos discriminatorios, e implementar medidas de mitigación de riesgos adoptadas.

Asimismo, en este clase de finalidades de implementación de la IA, conforme al principio de autonomía human, las medidas de supervisión cobran una especial importancia, ello por un lado, ante la difícil detección de casos discriminatorios, sobre todo cuando se trata de la discriminación por autoaprendizaje de la IA (que es información que no puede ser encontrada ni en los datos de desarrollo ni entrenamiento) y, por otro lado, ante el fácil acceso a grandes cantidades de datos proveídos por el BD y de identificar si el algoritmo está utilizando algún dato personal o

sensible sin el debido consentimiento, o si ha inferido por su cuenta algún rasgo personal o sensible y utilice tal información para tomar la decisión de a quién contratar para un determinado puesto laboral. Por tanto, se establece en el artículo 14 del Reglamento de Inteligencia Artificial, de la legislación europea, la supervisión humana sobre los sistemas de IA de alto riesgo durante todo el periodo que estén en uso, estableciéndose en su inciso 4 la posibilidad de descartar, invalidar o revertir sus resultados finales, así como la posibilidad de interrumpir intempestivamente su funcionamiento.

Así pues, de la revisión de los proyectos de ley y la legislación comparada podemos identificar una importante preocupación en que nuestro comportamiento entorno a los sistemas de IA sea moral, en cuanto existe una importante influencia ética en el establecimiento de medidas legislativas que regulan el uso de los sistemas de IA a nivel global, los cuales adoptan como vía de inicio un enfoque basado en principios éticos, que se complementa posteriormente con uno basado en potenciales riesgos del uso de la IA, estableciéndose pautas de comportamiento que debemos prever en cuanto al desarrollo y uso de la tecnología de la IA, que nos continuarán siendo de utilidad para que su constante proceso evolutivo vaya en armonía a su dimensión ética y continúe al servicio de la humanidad.

IV. Conclusiones

- a. La relación jurídico laboral es una necesariamente asimétrica en la que el derecho laboral asumirá un rol protector para con la parte más débil: el trabajador.
- b. El uso de la IA como herramienta de selección de personal puede afectar el derecho a la privacidad de los postulantes ante el acceso de fuente indirecta de datos personales o sensibles del postulante.
- c. El uso de la IA como herramienta de selección de personal puede afectar el derecho a la no discriminación de los postulantes, pudiendo generarse ello a lo largo de todo el ciclo de funcionamiento de la IA.
- d. A la fecha, a nivel internacional, legislaciones y proyectos normativos coinciden en establecer al uso de la IA como herramienta de selección de personal como uno de alto riesgo que obliga el cumplimiento de obligaciones adicionales específicas para su utilización.

La positivización constitucional de los neuroderechos en el ordenamiento jurídico peruano

Francisco Aspillaga Muñoz*

Resumen. – El avance de la neurotecnología, al intervenir directamente en la actividad cerebral, genera desafíos jurídicos que exigen una nueva respuesta normativa. En este contexto surgen los neuroderechos, una categoría emergente de cuarta generación orientada a resguardar la injerencia de la tecnología en la mente. Si bien su desarrollo aún es incipiente, con Chile como pionero en reconocerlos constitucionalmente, se propone su incorporación en el ordenamiento constitucional peruano para garantizar la autonomía personal frente al impacto de las tecnologías neurocognitivas.

Palabras clave.– Neurotecnología – Neuroderecho – Derecho humano.

Abstract.– Advances in neurotechnology, by directly intervening in brain activity, generate legal challenges that require a new regulatory response. In this context, neuro-rights have emerged, an emerging fourth-generation category aimed at protecting the mind from technological interference. Although their development is still in its infancy, with Chile as a pioneer in recognizing them constitutionally, their incorporation into the Peruvian constitutional order is proposed to guarantee personal autonomy in the face of the impact of neurocognitive technologies.

Keywords.– Neurotechnology – Neurolaw – Mental Integrity.

* Abogado por la Universidad Católica Santo Toribio de Mogrovejo, magister en Auditoría y Gestión Pública por la Universidad Católica de Trujillo, egresado de la maestría en Derecho Constitucional por la Universidad Privada Antenor Orrego. Fue asesor parlamentario, former ODS Ambassador en el programa Misión 2030 de la Organización de las Naciones Unidas. Actualmente es docente universitario y dirige el Estudio Jurídico Aspillaga & Asociados.

I. Introducción

El desarrollo acelerado de la neurotecnología —conjunto de herramientas capaces de registrar, modificar o influir en la actividad cerebral— plantea desafíos inéditos para el Derecho, especialmente en lo referente a la protección de la privacidad mental, la autonomía individual y la identidad personal. Estas nuevas realidades tecnológicas evidencian vacíos normativos que afectan directamente la dignidad humana, fundamento de todo sistema de derechos.

En este contexto, surge la figura de los neuroderechos como una propuesta jurídica orientada a reconocer nuevas formas de protección frente al uso potencialmente invasivo de tecnologías neurocognitivas. No obstante, en el Perú, estos derechos aún no han sido reconocidos expresamente ni constitucional, ni legal, ni jurisprudencialmente.

El objetivo principal de este artículo es analizar si los neuroderechos deben ser positivizados dentro del ordenamiento jurídico peruano como derechos constitucionales, fundamentales y humanos. Para ello, se parte de la hipótesis de que la incorporación explícita de estos derechos en el texto constitucional es necesaria para garantizar una protección efectiva de la mente en la era digital.

La metodología empleada es jurídico-dogmática y descriptiva, con base en el análisis normativo del derecho comparado y el estudio doctrinario. Asimismo, se acude al marco internacional de derechos humanos para fundamentar el carácter universal y progresivo de los neuroderechos.

La presente investigación se desarrolla en cuatro partes: primero, se revisan los conceptos y alcances de los derechos constitucionales, fundamentales y humanos; luego, se examina el vínculo entre Derecho y neurotecnología; en tercer lugar, se analiza la evolución y propuestas normativas de los neuroderechos a nivel global y regional; y, finalmente, se plantean conclusiones y recomendaciones concretas para su inclusión en el ordenamiento peruano.

II. Derechos Constitucionales, fundamentales y humanos

Para comprender adecuadamente el valor jurídico de los neuroderechos, es indispensable partir de las nociones básicas sobre los derechos constitucionales, humanos y fundamentales. Estos conceptos, aunque estrechamente vinculados entre sí, presentan distinciones clave que

permiten delimitar su alcance, origen y fuerza normativa. A continuación, se explican sus diferencias y relaciones para establecer el marco teórico que sustenta la necesidad de incorporar esta nueva categoría de derechos – los neuroderechos – en el ordenamiento jurídico nacional:

- Los **derechos constitucionales** son los “reconocidos –expresa o implícitamente– en la Constitución”¹
- Los **derechos fundamentales** son aquellos derechos humanos que han sido positivizados a nivel constitucional, es decir, están reconocidos y protegidos en una Constitución.²
- Los **derechos humanos** son aquellos inherentes a toda persona humana, sin ningún tipo de distinción, pues derivan de la dignidad humana como expresión de su naturaleza humana. Además, constituyen una fuente *per se* del derecho internacional, sirviendo de base para la firma de diversos instrumentos internacionales que reconocen y garantizan estos derechos.

i. Derechos Fundamentales

Los derechos fundamentales surgen de un proceso histórico y cultural de reconocimiento jurídico por parte del Estado, sustentado en normas emitidas por autoridad competente y positivizadas en la Constitución. Son exigibles judicialmente mediante mecanismos como el amparo o el hábeas corpus, con eficacia directa y efectos legales concretos. Son oponibles a todos, con límites legales definidos, y funcionan como libertades o derechos específicos. Poseen rango constitucional y forman parte del derecho positivo desde su reconocimiento por el sistema jurídico nacional.³

Para determinar si un derecho es fundamental, deben considerarse tanto su reconocimiento legal (criterio formal) como su importancia para la dignidad humana (criterio material). El **primer criterio** considera su

¹ CASTILLO, L. (2014). El Significado Del Contenido Esencial De Los Derechos Fundamentales. *Foro Jurídico*, No. 13, pp. 143-154, p. 143.

² Esa es la definición en el derecho positivo italiano y alemán. FERRAJOLI, L (2006). Sobre los Derechos Fundamentales. *Cuestiones Constitucionales*, No. 15, julio-diciembre, pp. 113-136.

³ HUERTA, C. (2010). Sobre la Distinción entre Derechos Fundamentales y Derechos Humanos. *Revista del Centro Nacional de Derechos Humanos*, No. 14, pp. 69-86.

reconocimiento dentro del ordenamiento jurídico, ya sea porque figura en el texto constitucional, en tratados internacionales con rango normativo, o ha sido declarado como tal por el Tribunal Constitucional. El **segundo criterio** evalúa si el derecho protege la autonomía y discernimiento de la persona, cubre necesidades básicas o garantiza igualdad en el acceso a libertades esenciales. Ambos criterios son importantes, pero en caso de conflicto, prevalece el criterio material, ya que la prioridad es salvaguardar la dignidad humana.⁴

ii. Antecedentes Históricos de los Derechos Humanos

El concepto de derechos humanos es resultado de las transformaciones sociales a lo largo del tiempo y refleja los cambios históricos.⁵ Por tanto, se puede afirmar que los derechos humanos son el resultado de una conquista histórica y social, que reconoce la dignidad, la libertad y el valor de toda persona, y establece las condiciones mínimas necesarias para vivir con dignidad.⁶

Los derechos humanos, tal como los concebimos hoy, nacieron tras la Segunda Guerra Mundial como respuesta a las graves violaciones cometidas durante el conflicto. Con el fin de evitar que estas atrocidades se repitieran, se fundó la Organización de las Naciones Unidas (ONU) en 1945 y, en 1948, se aprobó la Declaración Universal de los Derechos Humanos (DUDH). Aunque no tiene fuerza legal vinculante, esta declaración sentó las bases para los tratados internacionales en la materia, reconociendo derechos esenciales como la vida, la igualdad, la libertad de pensamiento y expresión, así como derechos sociales como el trabajo, la salud y la educación.⁷

⁴ Los criterios siguen la lógica del sistema jurídico español. BERNAL, C. (2015). Derechos Fundamentales. En J. Fabra & V. Rodríguez (Eds.), *ENCICLOPEDIA DE FILOSOFÍA Y TEORÍA DEL DERECHO*, pp. 1574-1591. Instituto de Investigaciones Jurídicas, UNAM.

⁵ Instituto Interamericano de Derechos Humanos. (2008). Campaña Educativa Sobre Derechos Humanos de las Personas Afrodescendientes. Módulo I: El Derecho a la Protección, p. 11.

⁶ UNICEF. (2022). El Enfoque Basado en los Derechos de la Niñez. Santiago de Chile, pp. 3-4. Obtenido en www.unicef.org/chile/media/7021/file/mod%201%20enfoque%20de%20derechos.pdf

⁷ *Idem*.

iii. Antecedentes Históricos de los Derechos Humanos

Los derechos humanos, se basan en la naturaleza y dignidad del ser humano según la tradición iusnaturalista y tienen como fuente positivizada primigenia a los tratados internacionales para declarar su reconocimiento, sin embargo, son preexistentes al ordenamiento jurídico positivo, y su protección, desde el realismo jurídico, depende de la voluntad estatal e instituciones internacionales.⁸

Según la Conferencia de Viena de 1993, los derechos humanos, sin importar su generación⁹, deben ser tratados con igual importancia¹⁰ porque pertenecen a todas las personas por su dignidad humana, sin distinción alguna, y su vigencia no depende de factores como nacionalidad, raza, sexo, condición social u otras¹¹, y poseen las siguientes características¹²:

- **Inherentes:** Son innatos a todos los seres humanos desde el nacimiento, sin necesidad de reconocimiento estatal. Constituyen la base de todos los derechos.
- **Universales:** Se aplican a toda la humanidad en cualquier lugar y momento; ningún factor justifica su desconocimiento.
- **Inalienables:** Son irrenunciables e inseparables de la persona humana; no pueden transferirse ni abandonarse.
- **Imprescriptibles:** No se pierden con el paso del tiempo, incluso si no se ejercen.
- **Indivisibles:** No hay jerarquías entre ellos; no se puede priorizar unos sobre otros ni sacrificar unos en beneficio de otros.

⁸ HUERTA, C. (2010). Sobre la Distinción entre Derechos Fundamentales y Derechos Humanos. *Revista del Centro Nacional de Derechos Humanos*, No. 14, pp. 69-86.

⁹ Las generaciones de los derechos las abordaremos en el siguiente apartado.

¹⁰ Instituto Interamericano de Derechos Humanos. (2008). Campaña Educativa Sobre Derechos Humanos De Las Personas Afrodescendientes Elementos Básicos De Derechos Humanos: Guía Introductoria. pp. 35-36. Obtenido en <http://biblioteca.corteidh.or.cr/tablas/26159.pdf>

¹¹ *Ibid.*, p. 10.

¹² *Ibid.* p. 36 y UNICEF (2015). Introduction to the Human Rights Based Approach: A Guide for Finnish NGOs and their Partners, p. 15. Obtenido en https://unicef.studio.crasman.fi/pub/public/pdf/HRBA_manuaali_FINAL_pdf_small2.pdf

- **Indisolubles:** Constituyen un conjunto inseparable; todos deben ejercerse en su esencia y tienen igual valor.
- **Interdependientes e interrelacionados:** El ejercicio de un derecho depende muchas veces del cumplimiento de otros. Por ejemplo, salud y educación.
- **Igualdad y no discriminación:** Todas las personas tienen los mismos derechos, sin importar raza, sexo, edad, religión, origen, discapacidad u otras condiciones.
- **Irreversibles:** Una vez que un derecho es reconocido como humano, no puede dejar de serlo en el futuro.
- **Progresivos:** Pueden ampliarse con el tiempo; pueden surgir nuevos derechos necesarios para preservar la dignidad humana.
- **Absolutos:** Su respeto puede exigirse frente a cualquier persona o autoridad, sin excepción.
- **Inviolables:** Nadie puede legítimamente actuar en contra de ellos, salvo por límites justificados en nombre del bien común.
- **Participación e inclusión:** Toda persona tiene derecho a intervenir activamente en la vida política, económica, social y cultural de su comunidad.
- **Rendición de cuentas y Estado de Derecho:** El Estado y otras autoridades deben respetar y garantizar los derechos humanos. Si no lo hacen, las personas pueden exigir justicia y reparación.

iv. Generaciones de los Derechos Humanos

La DUDH de 1948, el Convenio Europeo de Derechos Humanos (CEDH) de 1950 y la Convención Americana sobre Derechos Humanos (Pacto de San José) de 1969 han sido fundamentales para fortalecer el sistema internacional de derechos humanos. Su relevancia jurídica ha permitido el desarrollo de otras normas internacionales y ha dado origen a la clasificación de los derechos humanos en generaciones, según su aparición histórica. En el Perú, la DUDH cumple un rol fundamental, pues establece los estándares universales para interpretar, regular y aplicar los derechos humanos. Estos han sido incorporados al ordenamiento constitucional mediante el artículo 55° y la Cuarta Disposición Final y Transitoria de la Constitución peruana, formando parte del Bloque de Constitucionalidad y sirviendo como criterio interpretativo clave para garantizar los derechos y libertades reconocidos en la Ley Superior.

La **primera generación** de derechos humanos comprende los derechos civiles y políticos, que protegen la libertad, la vida y la participación política, exigiendo al Estado una actitud pasiva; la **segunda generación** abarca los derechos económicos, sociales y culturales, como el trabajo, la salud y la educación, que requieren intervención activa del Estado; y la **tercera generación** incluye los derechos colectivos o de solidaridad, como el derecho a la paz, al desarrollo y al medio ambiente, que demandan cooperación internacional.¹³

Los derechos humanos de **cuarta generación** tienen naturaleza híbrida entre lo científico y lo jurídico¹⁴ porque responden a los desafíos del avance tecnológico, especialmente en inteligencia artificial, biotecnología y neurociencias, protegiendo aspectos como la privacidad mental, la identidad personal y la autodeterminación. Se sustentan en instrumentos internacionales como las declaraciones de la UNESCO de 1997¹⁵, 2003¹⁶ y 2005¹⁷, que promueven una ética científica centrada en el ser humano y las generaciones futuras. En este contexto, **los neuroderechos forman parte de esta cuarta generación** y surgen como principios fundamentales que exigen garantías jurídicas claras ante tecnologías aplicadas al cerebro. Frente a la falta de regulación y el poder creciente de las corporaciones, se hace urgente que el Derecho evolucione para proteger efectivamente a la persona en esta nueva era digital.¹⁸

Los neuroderechos constituyen una propuesta emergente de derechos orientados a proteger la mente humana frente a posibles afectaciones derivadas del uso de neurotecnologías. Considerados partes de una nueva generación de derechos humanos, su objetivo es establecer un

¹³ RIVERA, K. (2019). *Los Derechos Humanos y las Limitaciones para su Protección en el Derecho Internacional*. Tesis para optar el título de abogado. Universidad Nacional Daniel Alcides Carrión, pp. 59-65.

¹⁴ IENCA, M. & ANDORNO, R. (2021). Hacia Nuevos Derechos Humanos en la Era de la Neurociencia y la Neurotecnología. *Análisis Filosófico* (41), pp. 177-179.

¹⁵ Declaración Universal sobre el Genoma Humano y los Derechos Humanos.

¹⁶ Declaración Internacional sobre los Datos Genéticos Humanos.

¹⁷ Declaración sobre Bioética y Derechos Humanos.

¹⁸ AMEZÚA, L. (2023). *Los Neuroderechos*. Universidad de Valladolid, pp. 47-61.

marco jurídico específico que garantice la integridad cerebral y regule éticamente estos avances científicos.¹⁹

III. Derecho y Neurotecnología

Etimológicamente la palabra **tecnología** está conformada por la palabra griega *téchne* (referente a técnicas u oficios) y *logos* (cuyo significado es conocimiento). Por tanto, podemos definir a la tecnología como el “conjunto de teorías y de técnicas que permiten el aprovechamiento práctico del conocimiento científico”²⁰; es decir, la tecnología es la aplicación del conocimiento para el desarrollo en sociedad, y es que, todas las tecnologías, desde la más rudimentaria hasta la actual y futurista, siempre han tenido, tienen y tendrán un impacto en la capacidad relacional humana, por tanto, “la tecnología debe ser considerada una construcción histórica”²¹ porque siempre forma parte del acontecer humano y como tal se encuentra ligada a las regulaciones jurídicas que puedan generarse por el nacimiento de la misma.

En tal sentido, es preciso afirmar que la tecnología influye en las relaciones humanas, pues, si la persona humana tiene una condición ontológica de sociabilidad, también podemos afirmar, sin lugar a dudas, que la irrupción tecnológica reconfigura la manera en que la sociedad interactúa, lo cual nos lleva a plantearnos la siguiente pregunta: *¿En pleno siglo XXI alguien puede vivir sin tecnología?*

La tecnología no se limita solo a lo digital; abarca todo uso del conocimiento científico para mejorar nuestras capacidades o superar limitaciones. Desde inventos simples como el fuego hasta sistemas complejos como las computadoras, cualquier herramienta o método que facilite y optimice nuestra vida diaria, académica, laboral, productiva o de cualquier índole, es tecnología, pues transforma y mejora las formas de hacer las cosas²²; lo que resalta el carácter histórico de la tecnología,

¹⁹ ALCAYAGA, C. (2024). *Neuroderechos: Protección por el Uso de Neurotecnologías*. Universidad de Chile, p. 23.

²⁰ REAL ACADEMIA ESPAÑOLA: Diccionario de la lengua española, 23.^a ed.

²¹ GÓMEZ, H. (2021). El Surgimiento Histórico de la Tecnología: Repercusiones en los Procesos De Investigación. *Revista Visión Electrónica*. Año 5. No. 1, pp. 123-132.

²² BORROMEIO, C. (2023). *¿Qué es la Tecnología?*. AZCATL. *Revista de divulgación en ciencias, ingeniería e innovación*, pp. 7-8.

destacando que cada etapa de la globalización —paleolítica, neolítica, ecuestre, clásica, oceánica, industrial y digital— refleja no solo un avance tecnológico y organizativo, sino también la aparición de nuevos desafíos y tensiones inherentes a dichos progresos²³, donde, evidentemente, el derecho juega un papel crucial por las regulaciones jurídicas que se originan como consecuencia del avance tecnológico.

En tal sentido, considerando la característica histórica de la tecnología, se puede afirmar que somos un *HOMO TECHNOLOGICUS*, es decir, somos una especie que está relacionada directamente con el mejoramiento de su entorno como consecuencia del darwinismo ontológico que nos impulsa a querer sobrevivir adaptando el espacio en el cual vivimos o generando herramientas que nos permitan adaptarnos a nosotros, lo cual se aplica en todos los ámbitos en el cual se desarrolla el ser humano y que abarca todas las ciencias usadas por la humanidad.

El ser humano es un ser social que no puede prescindir del medio en que vive²⁴ y es un ser que tiene una relación inherente con la tecnología en diferentes facetas, por ejemplo, hablamos del **ser-necesario** para señalar que el ser humano no puede evitar crear tecnología para sobrevivir, adaptarse y transformar su entorno; del **ser-saber**, porque la tecnología constituye un conjunto de conocimientos práctico y teórico que nos permite saber el cómo, por qué y para qué, así como la posibilidad de transmitir y mejorar los saberes; del **ser-acción**, ya que la tecnología representa una manifestación de la actividad humana en su relación con el mundo; y, por último, del **ser-sensible**, porque la tecnología genera en nosotros experiencias sensibles de belleza, armonía, forma y diseño como manifestación de nuestra creatividad.²⁵

²³ SACHS, J. (2021). *Las Edades de la Globalización: Geografía, Tecnología e Instituciones*. Barcelona: Deusto.

²⁴ RUEDA, J. (2007). La Tecnología en la Sociedad del Siglo XXI: Albores de una Nueva Revolución Industrial. *Aposta: Revista de Ciencias Sociales*, pp. 1-28.

²⁵ ESPARZA, R. & RUBIO, J (2016). *¿Qué Es Tecnología? Una Aproximación desde la Filosofía: Disertación en dos Movimientos*. Universidad de Costa Rica. *Revista Humanidades*, pp. 1-43.

La tecnología se desarrolla gracias a la transversalidad del conocimiento que es interdisciplinario, lo que demuestra su “contingencia e historicidad”²⁶, pues, la verdad basada en el conocimiento no es absoluta ni inmutable y el desarrollo de la misma es una manifestación de diferentes construcciones humanas influenciadas por aspectos culturales, sociales, políticos y jurídicos ya determinados que, *mutatis mutandis*, se adaptaron sobre la marcha a las nuevas realidades y contextos causados por el hombre y/o por la naturaleza, lo cual demuestra por qué la humanidad, a pesar de ser la criatura más débil y más co-dependiente de sus semejantes, hoy domina el mundo, y es que, el conocimiento desarrollado por la ciencia que genera tecnología no crece de manera lineal sino exponencial²⁷ con impacto directo e indirecto en el devenir del *homo sapiens* y del *homo sapiens sapiens*.

La tecnología, como manifestación del pensamiento humano, ha estado presente desde siempre. No obstante, su aplicación actual provoca una transformación en las relaciones entre los derechos y las instituciones políticas, generando un nivel de dinamismo sin precedentes y aún poco explorado.²⁸ Por tanto, el Estado, como garante del interés general, debe generar regulaciones jurídicas para asegurar que el desarrollo tecnológico proteja los derechos de la persona humana y el respeto de su dignidad.²⁹

²⁶ MORALES, G; RODRÍGUEZ, A. & SAURY, C. (2021). Clasificación de las Ciencias y Otras Áreas del Conocimiento, Una Problematicación. *Revista de investigación educativa de la Rediech*, pp. 1-22.

²⁷ Un claro ejemplo del crecimiento exponencial es la imprenta de tipos móviles de Gutenberg, inspirada en la tecnología china y difundida gracias al desarrollo comercial y tecnológico de la Ruta de la Seda, que permitió una expansión sin precedentes del conocimiento. Esto facilitó la validación científica del heliocentrismo, pero también provocó reacciones jurídicas como el juicio inquisitorial contra Galileo. Este caso ilustra cómo los avances tecnológicos y científicos pueden entrar en conflicto con el derecho y las estructuras socioculturales de su tiempo. Visto desde la actualidad, en plena era del conocimiento, resulta insólito que se haya perseguido a alguien por defender ideas como el heliocentrismo, del mismo modo que hoy sorprenden posturas como el terraplanismo o el antivacunismo.

²⁸ TENORIO, M. (2021). Tecnología y Constitución. *Revista de Derecho* (56), p. 117-134.

²⁹ LANDA, C. (2021). Constitución, Derechos Fundamentales, Inteligencia Artificial y Algoritmos. *THEMIS Revista De Derecho* (79), p. 37-50.

Lo que antes parecía ciencia ficción, hoy es posible, barato y común. Herramientas como la informática, las redes y la realidad virtual permiten a las personas desarrollar una identidad y ejercer derechos también en entornos digitales, desafiando los marcos tradicionales del derecho constitucional. Ante esta nueva realidad, urge definir con claridad los valores y alcances jurídico-constitucionales para construir respuestas sólidas y adecuadas³⁰, más aún si actualmente ya contamos con neurotecnología que puede redefinirnos como seres humanos.

Se entiende por **neurotecnología** a:

Todo desarrollo que permite monitorear o modificar el funcionamiento cerebral. De tal manera, la neurotecnología deriva en un conjunto de herramientas que sirven para manipular, registrar, medir y obtener información del cerebro, con el fin de analizar e influir sobre el sistema nervioso del ser humano”³¹, también se define como “el conjunto de métodos, herramientas o dispositivos que registran o modulan la actividad del sistema nervioso. Estos dispositivos pueden ser eléctricos, ópticos, magnéticos, acústicos, nanotecnológicos o químicos, y ahora se combinan con inteligencia artificial y redes neuronales profundas³².

Como hemos visto, la tecnología es uno de los motores del cambio social y forma parte de aquellos aspectos exógenos que influyen en la conformación del derecho de todas las sociedades, así tenemos que, el impacto sustancial del desarrollo tecnológico en el sistema jurídico que cada Estado posee es evidente, ya que, si existen más avances tecnológicos, se necesitan nuevos derechos relacionados directamente con la tecnología o con el uso de la misma.

³⁰ DÍAZ, F. (2008). La Constitución ante los Avances Científicos y Tecnológicos: Breves Reflexiones al Hilo de los Recientes Desarrollos en Materia Genética y En Tecnologías de la Información y la Comunicación. *Pensamiento Constitucional* (13), pp. 203-226.

³¹ BASTIDAS, Y. (2021). Neurotecnología: Interfaz Cerebrocomputador y Protección de Datos Cerebrales o Neurodatos en el Contexto del Tratamiento de Datos Personales en La Unión Europea. *Revista Iberoamericana de Derecho Informático* (11), pp. 101-176.

³² FUNDACIÓN INNOVACIÓN BAKINTER (2023). *Future Trends Forum: Neurotecnología para El Bienestar Humano*, p. 10. Obtenido en www.fundacionbankinter.org/wp-content/uploads/2023/10/Neurotecnologia-para-el-bienestar-humano-Fundacion-Innovacion-Bankinter.pdf

Por tanto, la tecnología, al ser una creación humana, no tiene voluntad propia, y su impacto positivo o negativo en la sociedad depende de cómo las personas decidan usarla³³, más aún si el avance de la tecnología ocurre a una velocidad que pocos habrían anticipado, por ello, resulta fundamental establecer mecanismos que permitan responder de manera ágil y eficaz ante eventuales vulneraciones de nuevos derechos humanos, fundamentales y/o constitucionales³⁴, que se desprenden de los avances neurotecnológicos y que dentro del positivismo jurídico mundial, ya tienen una categoría jurídica denominada neuroderechos.

IV. Los Neuroderechos: Del Mundo al Perú

i. Cuestiones Previas

El vertiginoso avance de las neurotecnologías, capaces de acceder, registrar e incluso modificar la actividad cerebral, plantea desafíos éticos y jurídicos sin precedentes, ya que estas tecnologías inciden directamente en el núcleo de la identidad humana: nuestras percepciones, recuerdos, emociones y decisiones. Su uso indebido pone en riesgo bienes fundamentales como la libertad, la autonomía, la privacidad mental y la dignidad personal, lo que impulsa la necesidad de reconocer los **neuroderechos** como una nueva generación de derechos humanos orientada a proteger la libertad cognitiva, la continuidad psicológica, la no discriminación algorítmica y el acceso equitativo al neuromejoramiento. En este contexto, la neuroética cumple un papel esencial al ofrecer criterios para evaluar los riesgos asociados al uso de estas tecnologías, y refuerza la urgencia de incorporar los neuroderechos en los marcos legales, constitucionales e internacionales, con el fin de salvaguardar la condición humana frente a posibles intervenciones abusivas³⁵ asegurando que el progreso científico respete la **dignidad humana**.

³³ MARIOS, J. & OSIMANI, J. (2005). *Tecnología I – EGB3. Proyecto Pedagógico con Modalidad a Distancia para la Terminalidad de Estudios de EGB3 y Educación Polimodal Editep*, pp. 63-64. Obtenido en https://bdigital.uncu.edu.ar/objetos_digitales/1397/tecno1egb3.pdf

³⁴ ROEL, L.; CHOCANO, E. & SALAZAR, P. (2023). Las Nuevas Tecnologías y el Daño al Derecho a la Autodeterminación Informativa y Derechos Conexos. La IA Como una Nueva Amenaza para los Derechos Fundamentales. *Tribunal Constitucional: Revista Peruana De Derecho Constitucional*, pp. 159-191.

³⁵ IRIARTE, C. (2021). Rafael Yuste, Neurobiólogo Profesor en la Universidad de Columbia, sobre Neuroderechos y el Planteamiento sobre su Reconocimiento y

Hoy en día, las neurotecnologías no solo registran y analizan la actividad cerebral asociada a conductas, emociones y funciones cognitivas, sino que también pueden intervenir en ella, modificando comportamientos, capacidades y estados emocionales³⁶, y es que, el avance de las neurociencias permite intervenir en el cerebro, generando dilemas éticos sobre privacidad, autonomía e identidad. Frente a ello, surgen los neuroderechos, propuestos para proteger la mente ante los riesgos de las neurotecnologías³⁷, por lo cual, estos nuevos derechos se enfocan en la: *i*) libertad cognitiva en su faceta positiva (poder acceder) y negativa (resistir a la tecnología sin consentimiento); *ii*) privacidad mental para proteger los datos contenidos y generados por nuestros cerebros; *iii*) integridad mental; y *iv*) continuidad psicológica, para que la persona mantenga su identidad de pensamiento, preferencias y elecciones habituales.³⁸

Cabe resaltar que, a raíz de los debates en la Universidad de Columbia, se propusieron cinco neuroderechos fundamentales que deberían incorporarse al marco internacional de derechos humanos: (1) el derecho a preservar la identidad personal frente a intervenciones que alteren el sentido del yo; (2) el derecho a la libertad de decisión, protegido ante manipulaciones tecnológicas; (3) el derecho a la privacidad de los datos neuronales, que exige consentimiento para su uso; (4) el derecho a la equidad en el acceso al mejoramiento cognitivo, evitando desigualdades; y (5) el derecho a la protección frente a sesgos algorítmicos, en especial los derivados de sistemas de inteligencia artificial no supervisados. Estas propuestas reflejan un debate ético y jurídico en expansión, dando lugar a campos como el *neurolaw*, que busca garantizar que el avance tecnológico respete la dignidad humana dentro de un marco legal adecuado.³⁹

Protección como Derechos Humanos. Obtenido en <https://anuariodh.uchile.cl/index.php/ADH/article/view/64448>

³⁶ PASCUAL-LEONE, A. Fundación Innovación Bakinter. Ob. Cit., p. 11.

³⁷ BORBÓN, D. & et al. (2023). El Preocupante Clausulado de la Ley Modelo de Neuroderechos del Parlatino. *Ius Et Scientia* (9) (2), pp. 228-260.

³⁸ RECHE, N. (2021). Nuevos Derechos frente a la Neurotecnología: La Experiencia Chilena. *UNED: Revista de Derecho Político*, pp. 415-446.

³⁹ CÁCERES, E. & LÓPEZ, C. (2022). *El Neuroderecho como un Nuevo Ámbito de Protección de los Derechos Humanos*. 2022, pp. 70-75.

ii. El Ordenamiento Jurídico Supraperuano

A nivel internacional, los neuroderechos están siendo abordados de forma diversa según el marco jurídico de cada país. Chile es el único que los ha reconocido a nivel constitucional. Argentina propuso regular su uso en investigaciones penales mediante control judicial previo y consentimiento informado. Uruguay y Colombia han iniciado debates legislativos, mientras que países como EE. UU., Francia, Italia, Finlandia, Grecia y España han optado por leyes ordinarias, jurisprudencia y estándares probatorios para proteger la intimidad mental y la libertad cognitiva. En varios de estos países ya se emplean neuropruebas en procesos penales, bajo estrictos límites. Esta diversidad de enfoques refleja una preocupación compartida por regular el impacto de la neurotecnología y garantizar la protección de la mente humana dentro del respeto al debido proceso y la dignidad.⁴⁰

La **Carta de Derechos Digitales de España**, a pesar de ser un documento de naturaleza declarativa y orientadora, tiene una importancia sustancial porque en su artículo XXVI menciona a los **neuroderechos** como parte del marco de derechos fundamentales en la era digital⁴¹, marcando un hito importante que impulsa la propuesta de que los neuroderechos pueden tener origen constitucional a través de distintas fuentes: jurisprudencia constitucional, reformas constitucionales, tratados internacionales con rango suprallegal, e incluso una eventual constitución global. Se plantea que los Estados constitucionales deben otorgarles rango constitucional general y sistematizarlos como límites al avance tecnológico, advirtiendo que su regulación tardía podría hacerlos ineficaces ante el completo desciframiento del funcionamiento cerebral.⁴²

⁴⁰ ACOSTA, B. (2024). La Constitucionalización De Los Neuroderechos Y Aplicación Del Principio Pro Homine En La Legislación Peruana. *Universidad Señor de Sipán*, pp. 53-83.

⁴¹ Gobierno de España. (2021). Carta de Derechos Digitales. Obtenido en <https://espanadigital.gob.es/lineas-de-actuacion/carta-de-derechos-digitales>

⁴² MASCITTI, M. (2022). El Rango Constitucional de los Neuroderechos como una Exigencia de Justicia. *Cuestiones Constitucionales (46)*, pp. 154-170.

iii. Los Desafíos de los Neuroderechos

El inexorable avance científico y tecnológico ha intensificado la preocupación por sus implicancias éticas y jurídicas, generando presión para establecer un nuevo régimen jurídico internacional. Estos desarrollos afectan no solo la vida social, sino también libertades fundamentales como la integridad física, la libertad individual y el pensamiento. En este contexto, el Derecho se ve forzado a expandir sus límites hacia una nueva y crucial frontera: la protección de la persona humana en el entorno tecnológico.⁴³

La construcción de los neuroderechos enfrenta cuatro desafíos clave; *i)* su definición conceptual, ya que provienen de debates neuroéticos con fuertes cargas filosóficas, lo que dificulta su claridad jurídica y consenso internacional; *ii)* sus implicancias éticas y culturales, especialmente respecto al acceso equitativo a tecnologías de mejora cognitiva no terapéutica, que puede chocar con visiones tradicionales y generar controversias sobre su financiamiento público; *iii)* su eficacia práctica exige evitar formulaciones que impongan cargas sociales o fiscales inasumibles; y *iv)* proteger la privacidad mental ante algoritmos sesgados plantea tensiones entre la precisión tecnológica y la intimidad personal. Abordar estos desafíos es esencial para que los neuroderechos sean conceptualmente claros, jurídicamente viables y socialmente legítimos.⁴⁴

El reconocimiento de los neuroderechos no debe quedar solo en manos del Poder Judicial y/o del Tribunal Constitucional, sino surgir de un proceso legislativo legítimo y abierto al debate público que permita crear una positivización de supuestos de hecho con consecuencias jurídicas de protección y sanción, asegurando así que el progreso científico respete la dignidad humana.⁴⁵ La intención de positivizar los neuroderechos a

⁴³ ORÍAS, R. (2022). Los Neuroderechos. Una Nueva Frontera para los Derechos Humanos. *Agenda Internacional* (40), pp. 211-227.

⁴⁴ BORBÓN, D. & MUÑOZ, J. (2024). El Neuroderecho a la Libertad Cognitiva: Fundamentos y Alcance de un Derecho Emergente. *Revista Ius Et Scientia*, pp. 112-113.

⁴⁵ ISLA, B. (2021). Los Derechos Fundamentales ante el Avance de las Neurotecnologías: ¿Es Necesario un Nuevo Catálogo De Derechos y Libertades?. 2021, pp. 19-46. Obtenido en www.repositorio.comillas.edu/xmlui/bitstream/handle/11531/49366/TFG%20Isla%20de%20la%20Vega%2c%20Belen.pdf?sequence=1&isAllowed=y

nivel interamericano, como respuesta a los desafíos éticos y jurídicos del avance neurotecnológico, la encontramos en la propuesta de **Ley Modelo de Neuroderechos para América Latina y el Caribe desarrollada por el Parlamento Latinoamericano y Caribeño (Parlatino)**^{46, 47}. Suma a esto, desde UNESCO se han propuestos los siguientes principios orientativos para los neuroderechos:⁴⁸

- **Adaptación normativa:** Los Estados deben actualizar sus leyes civiles, penales, laborales y procesales para enfrentar los desafíos de las neurotecnologías, garantizando la protección de los derechos fundamentales y promoviendo la responsabilidad de la industria desde el diseño.
- **Consentimiento informado y datos neuronales:** Toda recolección o uso de datos cerebrales requiere consentimiento libre e informado. Estos datos deben ser reconocidos como sensibles y protegidos con altos estándares de seguridad y encriptación.
- **Derecho a la privacidad mental:** Debe garantizarse que los datos mentales (pensamientos, recuerdos, emociones) no sean accedidos ni utilizados sin consentimiento expreso, protegiendo así la intimidad cognitiva de las personas.
- **Libertad cognitiva y autodeterminación:** Se debe evitar cualquier forma de manipulación mental mediante neurotecnologías. Las personas tienen derecho a pensar, decidir y actuar sin interferencias externas.
- **Derecho a la identidad personal:** La continuidad psicológica y el sentido del yo deben protegerse legalmente, impidiendo alteraciones de la personalidad sin consentimiento libre e informado, incluso en contextos médicos.

⁴⁶ El Parlatino es un organismo regional, permanente y unicameral, integrado por representantes elegidos por voto popular de los parlamentos de países soberanos de América Latina y el Caribe, incluido el Perú.

⁴⁷ Parlamento Latinoamericano y Caribeño. (2023). *Ley Modelo De Neuroderechos Para América Latina Y El Caribe*.

⁴⁸ ANDORNO, R. (2023). *Neurotecnologías y Derechos Humanos en América Latina y el Caribe: Desafíos y Propuestas de Política Pública*, pp. 34-37. Obtenido en <https://unesdoc.unesco.org/ark:/48223/pf0000387079>

- **Derecho a la integridad mental:** Se requiere una protección efectiva frente a daños neuronales o psicológicos causados por el mal uso de neurotecnologías, incluyendo sanciones civiles y penales ante hackeos o negligencias.
- **Prevención de la neurodiscriminación y sesgos algorítmicos:** Se deben evitar usos discriminatorios de datos mentales en ámbitos como empleo, seguros o educación, y regular los algoritmos que puedan amplificar desigualdades, sobre todo en grupos vulnerables.
- **Cautela ante el neuroenhancement:** Debe actuarse con prudencia ante tecnologías que buscan mejorar las capacidades mentales en personas sanas, ya que podrían generar ventajas injustas y ampliar brechas sociales.
- **Acceso equitativo a la neurotecnología en salud:** Los Estados deben garantizar que las neurotecnologías aplicadas a la salud sean accesibles para toda la población, especialmente en sectores empobrecidos o de difícil acceso.
- **Tutela efectiva de derechos neurotecnológicos:** No basta con reconocer estos derechos: deben existir mecanismos judiciales eficaces para protegerlos, incluso con figuras específicas como el *habeas mentem* o *habeas cogitationem*, que aseguren su defensa urgente.

El realismo jurídico nos enseña que, hasta el momento, el legislador ha confiado a los jueces la tarea de definir los alcances esenciales de los derechos fundamentales, especialmente en procesos de amparo o protección. Por ello, se requiere una adecuada capacitación de los operadores jurídicos, dado el rol clave que desempeñará la jurisprudencia en la interpretación y evolución de estos neuroderechos.⁴⁹

En tal sentido, el principio de unidad y separación del poder del Estado aquí cobra gran relevancia, porque, la **protección de los derechos humanos frente al uso de neurotecnologías es una responsabilidad primaria del Estado** y no solo de la comunidad internacional, cuyo rol es

⁴⁹ MARZUCA, Tarek. (2023). Neuroderecho: Análisis de la Ley N° 21.383 (Boletín N° 13.827) y el Boletín N° 13.828 Sobre Neuroprotección e Indemnidad Mental. *Universidad de Chile*, p. 118.

complementario. Corresponde a cada país **regular este campo según su realidad jurídica y social**, adaptando su marco normativo y permitiendo que su **jurisprudencia nacional contribuya activamente a la defensa de estos derechos emergentes**.⁵⁰ Para esto, es necesario abrir un debate interdisciplinario y nacional que permita diseñar marcos normativos sólidos, éticamente responsables y con garantías reales de protección⁵¹, siendo un primer paso, la constitucionalización de los neuroderechos en nuestro ordenamiento jurídico nacional.

Por tanto, como consecuencia de lo desarrollado, se puede afirmar que dentro del ordenamiento jurídico peruano, los neuroderechos deberían ser:

- Un **derecho constitucional** y por tanto ser positivizado en nuestra Carta Política como lo ha hecho Chile en el año 2021 a través de la Ley N° 21.383: “Modifica la Carta Fundamental, para establecer el desarrollo científico y tecnológico al servicio de las personas”⁵² pues, de esta forma, vamos a tener una progresión en la defensa de las libertades fundamentales.
- Un **derecho fundamental** porque cumple los criterios materiales de identificación que han sido desarrollados previamente.
- Un **derecho humano** por estar relacionado con la capacidad de autodeterminación humana sin injerencias que se desprende de su dignidad humana, las cuales han sido reconocidas implícitamente en la DUDH: *i*) En el artículo 1° se afirma la libertad y la racionalidad como base del ser humano, lo que fundamenta su capacidad de autodeterminarse; *ii*) Del artículo 3° se entiende que el derecho a la libertad es la base para ejercer la autodeterminación personal; *iii*) En el artículo 18° se reconoce la autonomía moral e intelectual, esencial para la autodeterminación; y *iv*) En el artículo 19° se protege la capacidad de cada persona para pensar, decidir y manifestarse libremente.

⁵⁰ ANDORNO, R. *Ob cit.*, p. 33.

⁵¹ BORBÓN, D. & et al. *Ob cit.*, p. 257.

⁵² Biblioteca del Congreso Nacional de Chile. Obtenido en <https://www.bcn.cl/leychile/navegar/imprimir?idNorma=1166983&idVersion=2021-10-25>

Por eso, si bien algunas críticas a los neuroderechos cuestionan su necesidad –alegando que el sistema actual de derechos humanos ya es suficiente y que existe una sobrevaloración de lo “neuro” –, también es cierto que la ampliación de derechos no es en sí negativa. La historia demuestra que nuevos derechos pueden fortalecer la protección jurídica, siempre que vayan acompañados de garantías efectivas, voluntad política y formación adecuada de los operadores jurídicos. El verdadero desafío no es evitar su reconocimiento, sino asegurar su eficacia real.⁵³

V. Conclusiones

- El avance de la neurotecnología plantea riesgos concretos para la autonomía, privacidad e identidad de las personas, afectando directamente la dignidad humana, lo que justifica la necesidad de una respuesta jurídica específica.
- Los neuroderechos representan una categoría emergente de derechos humanos de cuarta generación que buscan proteger la integridad mental y la libertad cognitiva frente a la intervención tecnológica, especialmente en contextos de inteligencia artificial, biotecnología y neurociencia.
- Aunque el ordenamiento jurídico internacional ha empezado a reconocer estos derechos de manera fragmentaria, solo Chile los ha incorporado expresamente a nivel constitucional, mientras que otros países exploran vías legislativas o jurisprudenciales para su protección.
- En el Perú, la positivización constitucional de los neuroderechos resulta jurídicamente viable y éticamente necesario, dado que cumplen con los criterios materiales y formales que justifican su constitucionalización.
- La regulación legal de los neuroderechos debe enmarcarse dentro de un proceso normativo que articule adecuadamente principios como la libertad cognitiva, la privacidad mental, la identidad personal, la equidad en el acceso a tecnologías y la protección frente a sesgos algorítmicos.

⁵³ DE ASÍS, R. (2022). Sobre la Propuesta de los Neuroderechos. *Universidad Carlos III de Madrid*, pp. 67-68. Obtenido en <https://e-revistas.uc3m.es/index.php/DYL/article/view/6873>

VI. Recomendaciones

- Incorporación constitucional: Se recomienda impulsar una reforma constitucional que reconozca expresamente los neuroderechos, tomando como referencia la experiencia chilena y adaptándola a la realidad peruana.
- Desarrollo legislativo integral: Es fundamental elaborar una ley marco sobre neuroderechos que regule el uso de neurotecnologías en contextos médicos, educativos, laborales y penales, garantizando el consentimiento informado y la protección de datos neuronales.
- Formación de operadores jurídicos: Se sugiere incluir contenidos sobre neuroderechos y derecho digital en los programas de formación y capacitación de jueces, fiscales, abogados y legisladores, a fin de dotarlos de herramientas para una adecuada interpretación y aplicación.
- Impulso del debate público interdisciplinario: Es necesario promover espacios académicos, científicos y legislativos donde converjan expertos en Derecho, neurociencia, ética y tecnología, con el fin de construir consensos sobre el alcance y regulación de los neuroderechos.
- Participación internacional activa: El Estado peruano debe participar activamente en foros y organismos internacionales, como la UNESCO o la OEA, para contribuir al diseño de estándares globales sobre neuroprotección y derechos digitales.

Smart contracts y Blockchain en la compraventa de inmuebles futuros: ¿el fin de las estafas en la etapa preventiva?

Luis Enrique Cabrera Chalán*

Resumen.- La compraventa de inmuebles futuros en etapa de preventiva presenta serias debilidades jurídicas estructurales en el Perú, al carecer de garantías efectivas sobre el uso de fondos. Este artículo propone incorporar smart contracts ejecutados en blockchain como mecanismo de auto ejecución contractual, capaz de reforzar la seguridad jurídica, asegurar hitos constructivos, mejorar trazabilidad financiera y reducir riesgos, todo ello dentro del marco normativo del derecho civil peruano.

Palabra clave.- Compraventa de bien futuro - garantías etapa de preventiva - smart contracts - blockchain - riesgos contractuales.

Abstract.- The sale of future real estate properties in the pre-sale stage presents serious structural legal weaknesses in Peru, as there are no effective guarantees regarding the use of funds. This article proposes incorporating smart contracts executed on blockchain as a mechanism for contractual self-enforcement, capable of reinforcing legal certainty, ensuring construction milestones, improving financial traceability, and reducing risks, all within the regulatory framework of Peruvian civil law.

Keywords.- Sale of future property - guarantees - pre-sale stage - smart contracts - blockchain - contractual risks.

* Abogado por la Universidad Nacional Mayor de San Marcos, egresado de la maestría de Derecho Civil y Comercial de la misma casa de estudios. Cuenta con especialización en Derecho inmobiliario, Derecho registral, Derecho notarial, Derecho administrativo y en Derecho digital y Legal Tech. Actualmente trabaja como abogado senior en Valderrama Abogados.

I. Introducción

La compraventa de inmuebles futuros es una práctica común en el Perú que ofrece ventajas económicas, pero también conlleva riesgos significativos. En la etapa de preventa, la falta de garantías legales sobre el uso de los fondos entregados por los compradores expone a estos a posibles incumplimientos o desvíos por parte del desarrollador. Esta ausencia de protección jurídica afecta la confianza en el sector y debilita la estabilidad del mercado inmobiliario.

El caso de Inversiones Piedra Alta, ocurrido en 2017, reveló graves irregularidades en la etapa de preventa inmobiliaria. Los compradores realizaron pagos significativos sin recibir las garantías adecuadas, mientras que la desarrolladora hipotecó los terrenos sin informarles, dejándolos en situación de vulnerabilidad jurídica¹. Este ejemplo evidencia la falta de mecanismos efectivos que aseguren el uso adecuado de los fondos en esta etapa, y resalta la necesidad de explorar herramientas tecnológicas, como los smart contracts, que podrían ofrecer mayor transparencia, trazabilidad y seguridad en las transacciones inmobiliarias.

A nivel legal, los compradores afectados enfrentan un panorama adverso, con derechos de propiedad y obligaciones contractuales en conflicto, y con escasas posibilidades de éxito en sede judicial. Esta situación evidencia la urgente necesidad de mecanismos jurídicos más eficaces para proteger al comprador en la etapa de preventa, donde sus compromisos económicos carecen de respaldo efectivo. La reiteración de casos de incumplimiento y fraude exige soluciones innovadoras acordes con los desafíos del mercado actual.

En ese marco, el presente artículo explora el potencial de las tecnologías disruptivas –en particular, los smart contracts ejecutados sobre plataformas *blockchain*– como herramientas para fortalecer la seguridad jurídica en la preventa inmobiliaria. Se plantea que estos mecanismos, al establecer cláusulas autoejecutables, pueden reducir el riesgo de incumplimiento y asegurar la trazabilidad de los fondos entregados. Asimismo, se analiza su viabilidad dentro del ordenamiento jurídico

¹ América Noticias, “Compradores estafados por constructora ocupan departamentos para no perder su inversión,” América Televisión, 30 de julio de 2023, <https://www.americatv.com.pe/noticias/actualidad/compradores-estafados-constructora-ocupan-departamentos-no-perder-su-inversion-n478772>.

peruano, así como los retos normativos y técnicos que su incorporación efectiva supone.

II. Iter contractual y principales riesgos que en la compraventa de bien futuro

i. Etapa inicial o etapa de preventiva

La etapa inicial o etapa de preventiva de la compraventa de bienes futuros se caracteriza por las tratativas directas entre el desarrollador inmobiliario y los potenciales compradores. Durante esta etapa, generalmente el proyecto inmobiliario se encuentra sin un banco sponsor, sin una titularidad inscrita en los registros públicos, u otra condición que se regulariza en las siguientes etapas. Es común que los desarrolladores inmobiliarios llevan a cabo negociaciones preliminares con los potenciales compradores, ofreciéndoles a cambio de aceptar estas condiciones del proyecto, precios con descuentos, inmuebles con mejores distribuciones o vistas, o tamaños más grandes, etc.

Luego, de las etapas de tratativas, cuando ya existe un acuerdo mínimo al menos en los elementos esenciales del contrato de compraventa de bien futuro², se suscribe un “acuerdo de separación” en virtud del cual los compradores realizan pagos iniciales o depósitos para separar el inmueble de su interés, estos montos de separación implican para el comprador un compromiso financiero significativo sin garantías tangibles sobre la ejecución del proyecto a cargo del desarrollador.

Luego, se suelen suscribir los contratos de compraventa de bien futuro, en los cuales se establecen un cronograma de pagos, estableciendo la forma de pago del precio de venta, en armadas o al contado; si es con crédito hipotecario (la forma más habitual), autofinanciamiento, y/o algún otro caso particular (dación en pago, permuta, etc). Nuevamente se presenta en la operación comercial, la falta de garantías efectivas sobre el destino de los flujos recaudados, que en la mayoría de los casos son depositados, transferidos y/o recepcionados de manera directa en las cuentas de los desarrolladores inmobiliarios.

² Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual. Resolución No. 3104-2018/SPC-INDECOPI, Exp. 0769-2016/CC2, 2018.

La Resolución Final No. 0034-2024/INDECOPI-LAM ilustra los riesgos de la etapa de preventa ante la ausencia de garantías sobre el uso de los fondos. En este caso, el comprador pagó más de S/108,000.00 directamente a la cuenta de la desarrolladora Grupo Unifica E.I.R.L., sin que se concretara la entrega de unos lotes. Ante la falta de respuesta y el cierre de las oficinas, el denunciante no logró contactarse con la empresa ni obtener información sobre el avance del proyecto. INDECOPI declaró fundada la denuncia por vulneración al derecho de información y ordenó la devolución del dinero. Este patrón se repitió en un caso similar la Resolución Final No. 0035-2024/INDECOPI-LAM), evidenciando una práctica que pone en riesgo las inversiones de los compradores por la falta de control sobre el destino de los fondos en preventa.

Los desarrolladores no están obligados por ley a destinar estos fondos exclusivamente a la ejecución del proyecto, lo que puede resultar en la desviación de los recursos hacia otros fines (publicidad, marketing, etc.) o incluso en la insolvencia del desarrollador (pago de otras acreencias, o créditos no relacionados al proyecto inmobiliario). Esta situación genera una gran incertidumbre para los compradores, quienes no tienen mecanismos efectivos para asegurarse de que su inversión será utilizada en la ejecución del proyecto inmobiliario.

ii. Etapa de Activación del proyecto

La activación del proyecto se produce una vez alcanzadas ciertas condiciones, como un número mínimo de ventas y autorizaciones necesarias. En esta etapa, el proyecto obtiene financiamiento —generalmente de un banco sponsor— que le brinda viabilidad comercial y permite iniciar la construcción. Este respaldo financiero está sujeto a la evaluación de la viabilidad del proyecto y del plan de negocio del desarrollador.

Generalmente, el desembolso del préstamo para la ejecución del proyecto edificatorio no se realiza en un solo acto, sino que es gradual (en varios hitos) conforme se evidencia el avance de la obra, ello con el fin de evitar que el promotor inmobiliario desvíe los fondos a otros fines distintos, poniendo en riesgo la culminación de la obra. Para verificar el avance de la obra, el contrato [de financiamiento] establece la participación de un Supervisor Técnico, elegido por el banco, pero cuyo costo lo asume la

inmobiliaria, este supervisor especializado será quien dé el visto bueno para la procedencia de los desembolsos graduales³.

Se ha señalado que, como todo proyecto, un proyecto inmobiliario requiere de una evaluación financiera, económica y legal que permita determinar su viabilidad; la cual incluye, principalmente, un análisis del entorno (oferta y demanda), un presupuesto (costos del proyecto y valor de las ventas), y un plan de marketing y de ventas. Todos estos son factores que el banco toma en consideración al momento de la medición de sus riesgos, a fin de decidir si es que otorgará o no el financiamiento para la construcción de un proyecto inmobiliario⁴.

El caso del Expediente No. 006923-2020 evidenció la relevancia de informar adecuadamente sobre la activación del proyecto inmobiliario. V Capital S.A. alegó haber cumplido con su deber de información, pero INDECOPI concluyó que no brindó datos suficientes sobre las condiciones del financiamiento bancario, aspecto clave para el cumplimiento del contrato y los plazos de entrega. La Sala confirmó que no se acreditó dicha información al comprador, resaltando que la activación del proyecto constituye un hito determinante en la ejecución del contrato de compraventa.

En muchos casos, los desarrolladores optan por establecer un fideicomiso como mecanismo de protección, asegurando que los fondos recaudados se destinen exclusivamente a la construcción del proyecto. Al ser administrado por un tercero independiente, este esquema reduce el riesgo de malversación, refuerza la seguridad financiera y fortalece la confianza de los compradores al garantizar el uso adecuado de su inversión.

iii. Ejecución del proyecto inmobiliario

La ejecución del proyecto inmobiliario corresponde a la fase constructiva conforme al cronograma pactado. Si la obra concluye oportunamente, se cumplen las condiciones técnicas y legales del contrato, lo que satisface a

³ KANASHIRO, B. y RUBÉN, C. *Aspectos legales del negocio inmobiliario de bienes futuros* (Lima: Jurista Editores, 2022), 45.

⁴ ARTEAGA REÁTEGUI, M. "El rol del banco como intermediario financiero para la adquisición de inmuebles dentro del marco de desarrollo de proyectos inmobiliarios," THEMIS Revista de Derecho, no. 83 (2024), 307.

los compradores y fortalece la reputación del desarrollador. Sin embargo, los retrasos —por causas financieras, técnicas o administrativas— generan incertidumbre y costos adicionales para los compradores tales como vivienda temporal o pagos de intereses. En estos casos, cobra relevancia el rol de INDECOPI como ente encargado de velar por los derechos de los consumidores inmobiliarios.

Por otro lado, la no conclusión del proyecto es la situación más crítica, donde la construcción se detiene indefinidamente o se abandona. Este escenario puede ser resultado de la insolvencia del desarrollador, problemas legales (actuaciones arbitrarias de la administración), o una mala gestión del proyecto. En tales casos, los compradores se enfrentan a la pérdida parcial o total de su inversión y la necesidad de recurrir a largos y costosos procesos legales para intentar recuperar su dinero o exigir el cumplimiento del contrato.

En resumen, la ejecución del proyecto inmobiliario es una etapa crucial que puede culminar de tres maneras: conclusión oportuna, conclusión no oportuna, o no conclusión. Cada uno de estos resultados tiene implicaciones significativas para los compradores y el desarrollador, destacando la necesidad de mecanismos de garantía y protección adecuados durante todo el iter contractual para mitigar los riesgos asociados y asegurar la transparencia y confianza en el proceso.

III. Mecanismos legales tradicionales

Ante la ausencia de garantías específicas en la etapa de preventa inmobiliaria, el ordenamiento jurídico ofrece ciertos mecanismos contractuales tradicionales que pueden emplearse para proteger los fondos entregados por los compradores. Estos mecanismos, aunque no son de uso obligatorio, han demostrado ser herramientas útiles para mitigar los riesgos asociados a la falta de control sobre el destino de los recursos antes de la activación del proyecto. A continuación, se describen principalmente el fideicomiso en garantía, la cuenta escrow y el contrato de depósito, sin perjuicio de que puedan existir otras figuras jurídicas que también cumplan una función similar en este contexto.

i. Fideicomiso en garantía

El fideicomiso de garantía es un acuerdo legal en el que un fiduciario, generalmente es una entidad financiera o un fiduciario designado,

administra y controla los fondos o activos en beneficio de los beneficiarios, en nuestro caso, los compradores inmobiliarios, conforme a los términos del contrato de fideicomiso.

Según Martorell, citado por Lama More (2012-2013, 50), el fideicomiso de garantía es aquel por el cual se transfiere al fiduciario bienes para garantizar con ellos o con su producto el cumplimiento de ciertas obligaciones a su cargo o a cargo de terceros, designando como beneficiario al acreedor o a un tercero en cuyo favor, en caso de incumplimiento, se pagará una vez realizados los bienes, el valor de la obligación o el saldo insoluto de ella, conforme a lo previsto en el contrato; refiere este autor que se trata de un sustituto práctico del tradicional sistema de garantías reales; la diferencia sustancial que existe con éstas, es que si bien se trata de la efectivización de la garantía en caso de incumplimiento, la venta fiduciaria no es una ejecución forzada, sino simple cumplimiento de una obligación alternativa⁵.

No es común que los proyectos inmobiliarios cuenten con un fideicomiso antes de su activación, pero su implementación en la etapa de preventiva brinda al comprador una mayor seguridad. Este mecanismo garantiza que los fondos se destinen exclusivamente a la construcción, mejora la transparencia mediante una gestión externa y reduce el riesgo de malversación por parte del desarrollador.

ii. Contrato de cuenta *escrow*

Según Carracedo Bottifoll, citado por Nakamura Velásquez (2009, 290), el contrato de escrow es aquel donde las partes convienen los pactos y condiciones para establecer una Garantía consistente en el depósito de saldos de efectivo u otros instrumentos en una cuenta especial administrada por una institución bancaria [escrow agent], que resultan ejecutables a favor del acreedor en caso de cumplimiento de una o varias condiciones previamente establecidas⁶.

Por otro lado, como se ha advertido, el problema con este tipo de operaciones [Fideicomiso en Garantía], es que la estructuración de esta

⁵ Citado en Héctor Enrique Lama More, "Garantías en títulos valores," *Revista Oficial del Poder Judicial*, año 6-7, núm. 8 y 9 (2012-2013): 56, citando a Martorell.

⁶ Citado en Dan Nakamura Velásquez, "El Escrow," *Derecho & Sociedad*, no. 33 (2009): 290, citando a Juan J. Carracedo Bottifoll.

requiere incurrir en altos costos, como los honorarios del fiduciario, asesoría legal, publicaciones, entre otros. Por el contrario, si bien el contrato de escrow no significa que el dinero consignado en dicha cuenta haya salido del patrimonio del agente que enajena los activos materia del contrato principal, con lo que no se obtiene la misma protección que con un fideicomiso en garantía, tiene la ventaja de que el banco que tiene en custodia los fondos paga intereses por el dinero que recibe y no se requiere incurrir en mayores costos⁷.

Aunque el fideicomiso y la cuenta escrow comparten ciertas similitudes, esta última es un contrato atípico, más sencillo y menos flexible, cuya regulación depende exclusivamente de lo pactado por las partes. A diferencia del fideicomiso, la liberación de fondos en el escrow se realiza conforme a condiciones previamente acordadas. Su implementación en preventas requiere un agente neutral que administre los fondos y verifique los hitos del proyecto, asegurando su uso exclusivo en la construcción y reduciendo riesgos para los compradores.

Es así como para implementar una cuenta escrow en la etapa de preventa, es necesario designar un agente neutral —como un banco o empresa especializada— que administre los fondos según un contrato pactado entre las partes, con condiciones basadas en hitos del proyecto. Los pagos de los compradores se retienen hasta que se verifique el cumplimiento de dichos hitos por un auditor o el propio agente. Este mecanismo asegura que los fondos se usen exclusivamente en la construcción, reduciendo el riesgo de desvíos y fortaleciendo la confianza en la operación inmobiliaria.

iii. El contrato de depósito

El artículo 1814 del Código Civil define el contrato de depósito como aquel en el que el depositario recibe un bien para custodiarlo y devolverlo a solicitud del depositante. Este contrato implica deberes de conservación y entrega, incluso antes del plazo pactado si no es en beneficio del depositario o un tercero. Existen dos escenarios: el depósito en interés del depositario y el celebrado a favor de un tercero. El primero podría aplicarse en preventas inmobiliarias como mecanismo alternativo de garantía frente a la falta de protección jurídica en dicha etapa.

⁷ *Ibid.*, 292.

Se ha indicado que, el contrato puede ser celebrado en interés del depositario. Esta disposición no debería ser entendida en caso el depositario sea retribuido. En efecto, el interés del depositario puede encontrarse en el supuesto de que el bien haya sido entregado por el depositante en custodia al depositario y a su vez, por existir una diferente relación crediticias precedente o contemporánea entre las mismas partes, se hubiese constituido una prenda sobre dicho bien a favor del mismo depositario. En este supuesto se tendría que especificar en el documento que contiene el contrato de depósito la necesaria referencia a que dicho acto se celebra en interés del depositario, acreedor prendario del mismo bien depositado⁸.

Así, este sería el caso, por ejemplo, que un comprador entregue una suma de dinero al desarrollador, en calidad de “depósito” y cuando sean cumplidos ciertos hitos esta suma de dinero sea entregada o “liberada” a su favor e interés, con lo cual dicha suma de dinero podrá ser imputada al pago de cuotas de la compraventa. Nótese que en el contrato de compraventa se podría pactar que el precio sea pagado en armadas de dinero que serán deducidas o imputables de la suma de dinero que haya sido entregado en calidad de depósito, cumpliendo ciertos hitos. Con ello, la constructora mantiene en su poder el dinero, y frente al cumplimiento de determinado evento (por ejemplo, obtención de licencia de obra) pueda liberar la suma de dinero a su favor.

IV. Tecnologías disruptivas aplicables: Smart Contracts y Blockchain

i. Conceptos y funcionamiento

La tecnología *blockchain* se trata de una estructura descentralizada y distribuida de almacenamiento de datos, que registra transacciones de forma inmutable y cronológica a través de una red de nodos interconectados. Esta tecnología garantiza la integridad, trazabilidad y seguridad de la información sin requerir de un intermediario central, lo

⁸ AMAYA AYALA, Luis. “Comentario al art. 1830 del Código Civil,” en Código Civil comentado, ed. Mario Muro Rojo y Marisol Torres Carrasco (Lima: Gaceta Jurídica, 2022), 325.

que la hace especialmente útil en contextos donde la confianza entre las partes es limitada⁹.

En este entorno, los *smart contracts* son programas informáticos que se ejecutan automáticamente en una *blockchain*, activándose cuando se cumplen determinadas condiciones predefinidas¹⁰. Esta auto ejecución elimina la intervención humana y reduce el riesgo de incumplimiento¹¹, lo cual resulta especialmente ventajoso en etapas sensibles como la preventa inmobiliaria. Una de las plataformas más utilizadas para su implementación es Ethereum, que permite no sólo transferencias de valor, sino también la creación de aplicaciones descentralizadas (DApps) y organizaciones autónomas (DAOs), sobre las cuales se ejecutan estos contratos inteligentes.

Una vez programado el código, el contrato queda inmutable en la red y opera sin posibilidad de modificación unilateral, garantizando un cumplimiento objetivo y automático. Entonces, debido a que el smart contract es autoejecutable e inmutable, el riesgo de contraparte o de incumplimiento sería igual a cero¹².

En ese contexto, los *smart contracts* puede ser utilizados, tal vez no en todo el iter contractual de la compraventa inmobiliaria, por cuanto finalmente, en la práctica encuentra limitantes tales como la formalidad

⁹ A modo ilustrativo, Corrales, Fenwick y Haapio presentan un ejemplo sobre una transferencia bancaria tradicional: “Take for instance a bank transaction. Imagine that a person called Anna would like to send money to another person called Bob [...] Both depend entirely on those banks (and their commissions) to carry out the transaction. What the Blockchain basically proposes is to eliminate intermediaries and decentralize the entire management system [...] This is why the Blockchain represents a profound paradigm shift in the entire financial structure that we currently use.” Véase Marcelo Corrales, Mark Fenwick y Helena Haapio, eds., *Legal Tech, Smart Contracts and Blockchain* (Singapore: Springer, 2019), 4.

¹⁰ Imran Bashir define los smart contracts como “a secure and unstoppable computer program representing an agreement that is automatically executable and enforceable.” Véase Imran Bashir, *Mastering Blockchain*, 2.^a ed. (Birmingham: Packt Publishing, 2018), 242.

¹¹ MORÁN, Alfredo. “El valor de la confianza: Introducción al uso de la tecnología blockchain (smart contracts, tokens) en el mercado de valores peruano” en *Derecho contractual financiero: Estudios en homenaje a la Facultad de Derecho PUCP en su centenario*, ed. Sergio García Long (Lima: Normas Jurídicas SAC, 2019), 312..

¹² *Ibid.*

de escritura pública, inscripción en los registros públicos, entre otras, pero si al menos en la actualidad, en la etapa de preventiva en la que generalmente solo se suscribe un contrato privado.

En el contexto de la suscripción de contratos de separación y el pago de las primeras armadas de dinero, el cumplimiento del cronograma de pago pactado entre las partes es esencial. En este escenario se advierten dos intereses fundamentales. Por un lado, la empresa constructora tiene un interés esencial en garantizar la captación sostenida de recursos para financiar la obra. Estos fondos son necesarios para financiar la construcción en curso, pagar a los proveedores y asegurar la continuidad del proyecto. Sin un flujo constante de capital, la constructora [o el desarrollador inmobiliario] podría enfrentar dificultades financieras que retrasen o incluso paralicen la obra¹³.

Por otro lado, el comprador tiene un interés legítimo y fundamental en que su dinero sea utilizado de forma efectiva y exclusiva para la ejecución del proyecto. No solo desea observar avances materiales en la construcción, sino también contar con la certeza de que su inversión está siendo gestionada adecuadamente. En ese sentido, la confianza en que los fondos aportados serán destinados exclusivamente a la obra es esencial, ya que ello incide directamente en la posibilidad de que el inmueble sea construido y entregado dentro del plazo pactado. Por ello, resulta indispensable que el desarrollador actúe con transparencia y brinde garantías sobre el uso de los recursos recaudados durante la preventiva.

Consideramos que, la utilización de los *smart contracts* puede solucionar ambos intereses al establecer reglas autoejecutables. Estos contratos digitales permiten programar y automatizar las condiciones pactadas, asegurando que los pagos se realicen de acuerdo con el cronograma establecido y que los fondos se utilicen de manera eficiente. Así, se garantiza que la constructora reciba los pagos necesarios para continuar

¹³ Un ejemplo ilustrativo es el caso de la empresa constructora ICA en México, que durante la crisis del sector en 2015 implementó diversas medidas para mantener su liquidez, como bursatilización de activos, recortes de gastos y traslado de deuda a nuevos proyectos, evidenciando su necesidad constante de captar recursos para garantizar la continuidad operativa. Véase Martínez-González, M., Saavedra-García, M. y Sánchez-Limón, M., "Modelo de proyección financiera para el sector construcción," *Lúmina* 22, n.º 1 (2021): 15.

la obra y que el comprador tenga la seguridad de que su dinero se está empleando correctamente en el proyecto.

ii. Diferencias y ventajas con los mecanismos tradicionales

Una de las principales diferencias entre los smart contracts y los mecanismos tradicionales de garantía radica en su naturaleza y funcionamiento. Mientras que el fideicomiso, la cuenta escrow y el contrato de depósito son figuras jurídicas reconocidas y ejecutadas dentro del marco normativo convencional, los smart contracts son programas informáticos que se ejecutan automáticamente en una plataforma *blockchain*, como Ethereum. Esta ejecución automática permite que las condiciones pactadas se cumplan sin necesidad de intervención humana ni validación posterior por parte de terceros, lo cual elimina en gran medida el riesgo de incumplimiento voluntario por una de las partes.

Otra diferencia importante es el grado de descentralización y transparencia que ofrecen los smart contracts. En los mecanismos tradicionales, la gestión de los fondos y el cumplimiento de condiciones dependen de terceros —como fiduciarios, agentes bancarios (escrow agent) o depositarios—, lo que implica mayores costos, necesidad de confianza en dichos intermediarios y posibles demoras operativas. En cambio, los smart contracts operan sobre una red distribuida e inmutable, lo que permite que todas las transacciones queden registradas públicamente en la *blockchain*, generando trazabilidad, seguridad y confianza sin necesidad de intermediación.

En cuanto a la eficiencia, los smart contracts ofrecen ventajas significativas respecto a los mecanismos tradicionales. Su capacidad de automatizar la ejecución de obligaciones contractuales permite reducir los tiempos de cumplimiento, minimizar errores humanos y eliminar la burocracia asociada a la verificación manual de condiciones. Por ejemplo, puede programarse que el desembolso de una armada de pago al desarrollador se realice únicamente cuando se confirme —a través de un oráculo o fuente externa confiable— que se ha alcanzado un determinado hito constructivo. Esta ejecución automática contrasta con lo que ocurre en mecanismos como el fideicomiso o la cuenta escrow, donde la verificación y liberación de fondos requiere la intervención de terceros, validación documental y procedimientos formales.

En este contexto, los oráculos (oracles) desempeñan un rol clave. Según Mekki, un oráculo es una persona, entidad o aplicación informática que conecta la *blockchain* con el mundo real, permitiendo que los smart contracts accedan a información externa necesaria para su ejecución¹⁴. Gossa añade que estos oráculos pueden ser profesionales del derecho, dispositivos físicos o programas informáticos encargados de recopilar, verificar y certificar datos relevantes del entorno físico, no contemplados en el contrato, pero determinantes para su cumplimiento. Gracias a ellos, se superan los límites de autoejecución inherentes a estos contratos inteligentes¹⁵.

Un ejemplo ilustrativo del funcionamiento práctico de los smart contracts es el que menciona la Law Commission del Reino Unido —recogido por Lupián Morfín— en relación con una póliza de seguro de viaje desarrollada como contrato inteligente. En este caso, el smart contract se encuentra vinculado a una base de datos global de tráfico aéreo, cuya información es suministrada por medio de un oráculo. Cuando el sistema detecta que un vuelo ha sufrido un retraso, dicha información es automáticamente transmitida al contrato inteligente, que ejecuta de inmediato el pago compensatorio al titular de la póliza. Todo el proceso ocurre sin necesidad de intervención humana, verificación manual o procesos adicionales de validación¹⁶.

Este ejemplo pone de manifiesto cómo los smart contracts, en combinación con oráculos confiables, pueden transformar la ejecución de obligaciones contractuales mediante sistemas automatizados, transparentes y eficientes. Si bien se trata de un supuesto del ámbito asegurador, su lógica puede extrapolarse al contexto inmobiliario —por ejemplo, en la etapa de preventiva de bienes futuros— para condicionar pagos u obligaciones a eventos verificables como la obtención de licencias, el

¹⁴ MEKKI, M.: *Le contrat, objet des smart contracts* (partie 2). 2019. Dalloz IT/IP, 1, 29.

¹⁵ GOSSA, J.: *Les blockchains et smart contracts pour les jurists*. 2018. Dalloz IT/IP, No. 7-8, 393-397.

¹⁶ LUPIÁN, G. Smart Contracts y Blockchain. Una nueva realidad contractual internacional, dir. Luis Manuel C. Méjan (Ciudad de México: Tirant lo Blanch, 2023), 43; citando Law Commission, *Reforming the Law: Smart Legal Contracts*, Advice to Government, Presented to Parliament by the Lord Chancellor and Secretary of State for Justice by Command of Her Majesty, November 2021, 21.

avance de obra o la conclusión de hitos constructivos, reduciendo así el riesgo de incumplimiento por parte del desarrollador. En este sentido, los smart contracts no solo constituyen una herramienta tecnológica, sino un instrumento jurídico disruptivo con capacidad de reforzar la seguridad contractual a través de medios digitales.

Finalmente, cabe destacar que los smart contracts, pese a su gran potencial, aún enfrentan ciertos límites frente a los mecanismos tradicionales. En el contexto peruano, su aplicabilidad puede verse restringida por exigencias legales como la formalidad de escritura pública, la necesidad de inscripción registral o la ausencia de regulación específica para contratos celebrados y ejecutados por medios digitales autónomos. No obstante, como mecanismo complementario en la etapa de preventa —donde las operaciones suelen realizarse mediante contratos privados—, los smart contracts representan una alternativa innovadora, eficiente y con un nivel de seguridad que supera en varios aspectos a las herramientas tradicionales.

iii. Propuestas de implementación de Smart contracts en la etapa de preventa

Para implementar smart contracts en la etapa de preventa inmobiliaria, lo primero es identificar qué obligaciones contractuales pueden ser digitalizadas y automatizadas sin contravenir normas imperativas del ordenamiento jurídico peruano. En esta etapa, predominan los contratos privados en los que se pactan pagos iniciales, cronogramas de armadas, condiciones para el inicio de obra, entre otros aspectos que son susceptibles de ser programados en el sistema de ejecución automatizada. Así, puede estructurarse un smart contract que, por ejemplo, libere automáticamente una armada de dinero a favor del desarrollador inmobiliario solo cuando se acredite el cumplimiento de un hito constructivo previamente definido.

Una forma práctica de implementar este sistema es a través de la integración de oráculos, que como se ha mencionado son aplicaciones que conectan datos del mundo real con la *blockchain*. Estos oráculos pueden actuar como verificadores externos del cumplimiento de hitos de obra, tales como la obtención de la licencia de edificación, la culminación del sótano, o la instalación de estructuras clave, conforme al cronograma del proyecto. Una vez que el oráculo certifica el cumplimiento de la condición, el smart contract ejecuta automáticamente la cláusula

correspondiente y autoriza la transferencia de fondos desde la cuenta del comprador o desde una cuenta escrow previamente vinculada¹⁷.

Asimismo, se recomienda que el uso de smart contracts en esta etapa vaya acompañado de medidas de seguridad legal complementarias, como la incorporación de cláusulas tradicionales de resolución, penalidades o garantías personales codificadas como condiciones dentro del contrato inteligente¹⁸. Esta combinación entre herramientas jurídicas tradicionales y tecnología puede brindar mayor confianza a las partes y facilitar una transición progresiva hacia modelos contractuales más digitales. Además, la participación de abogados con conocimientos en derecho y tecnología será clave para garantizar que la estructura del smart contract se ajuste al marco legal vigente y respete los principios generales del derecho contractual en el ordenamiento jurídico peruano.

Finalmente, es importante que el sector inmobiliario —junto con desarrolladores, abogados, notarios y entidades financieras— explore la posibilidad de establecer estándares o protocolos para el diseño y uso de smart contracts en operaciones de preventiva. Esta estandarización contribuiría a reducir costos de implementación, facilitar auditorías externas y promover la interoperabilidad entre distintas plataformas. Si bien su aplicación masiva aún enfrenta desafíos regulatorios y culturales, su implementación gradual y estratégica en la etapa de preventiva puede marcar un punto de inflexión en la modernización de la contratación inmobiliaria en el Perú.

¹⁷ Sobre la responsabilidad del *oracle* en caso de que se introduzca o procese información errónea, Mustapha Mekki plantea: “*As for the Oracle, which refers to the person who integrates external data into the blockchain, can it be held liable? If it is a natural or legal person, they should assume liability for erroneous or falsified information. If it is an Oracle algorithm, we should again ask ourselves whether the developer can be held liable even though it is open-source software, or consider the liability of intermediaries.*” Véase Nathalie Blanc y Mustapha Mekki, *Le juge et le numérique : un défi pour la justice du XXI^e siècle* (París: Dalloz, 2019), 28.

¹⁸ En un escenario de autoejecución mediante *smart contracts*, el incumplimiento no es deliberado, ya que la ejecución está automatizada. Sin embargo, si el comprador enfrenta circunstancias que afectan su capacidad de pago —como la denegatoria de un crédito hipotecario o una pérdida de ingresos— podrían activarse cláusulas previamente programadas que establezcan penalidades. Estas disposiciones funcionarían como mecanismos de salida limitados, diseñados para otorgar seguridad jurídica y previsibilidad a ambas partes.

iv. Ejemplos simulados de smart contracts en la preventa inmobiliaria

Con el fin de ilustrar la viabilidad técnica y práctica de los smart contracts en la etapa de preventa inmobiliaria, se presentan a continuación ejemplos simulados que muestran cómo pueden programarse cláusulas contractuales autoejecutables vinculadas al cumplimiento de hitos constructivos. En todos los casos, se parte del supuesto de que las partes celebran un contrato privado de compraventa de bien futuro, sujeto a condiciones objetivas verificables mediante oráculos previamente definidos.

En un primer ejemplo, las partes acuerdan que la primera armada del precio (equivalente al 20 %) se liberará únicamente cuando el desarrollador obtenga la Licencia de Edificación. El smart contract, codificado en la red Ethereum, se conecta a un oráculo que verifica periódicamente la base de datos de la municipalidad competente¹⁹ o valida un documento emitido por la autoridad edil. Una vez acreditado el cumplimiento del hito, el contrato ejecuta automáticamente la transferencia del monto a favor del desarrollador, asegurando que los fondos solo se utilicen cuando el proyecto haya alcanzado condiciones mínimas de viabilidad legal.

Un segundo supuesto se refiere al desembolso de una armada del 30 % del precio, condicionado a la culminación del primer nivel estructural del edificio. El cumplimiento de este hito debe ser certificado por el Supervisor Técnico mediante un informe suscrito (digital o físicamente), el cual es remitido al smart contract a través del oráculo correspondiente. Verificado el avance, se autoriza automáticamente la liberación del pago, asegurando que los fondos del comprador se apliquen de forma estricta al progreso real de la obra.

Estos ejemplos evidencian cómo los smart contracts permiten trasladar condiciones jurídicas al plano tecnológico, facilitando la ejecución automática de obligaciones contractuales y reforzando la transparencia, trazabilidad y eficiencia en la gestión de fondos durante la etapa crítica de preventa inmobiliaria.

¹⁹ De manera ilustrativa, en la Plataforma Nacional de Datos Abiertos, se puede observar cuáles son las licencias de Edificación que han sido otorgadas en el distrito de Miraflores: <https://datosabiertos.gob.pe/dataset/resoluci%C3%B3n-de-licencia-de-edificaciones-municipalidad-de-miraflores>

V. Desafíos y compatibilidad con el ordenamiento jurídico peruano

Actualmente, los smart contracts no cuentan con reconocimiento expreso en el ordenamiento jurídico peruano, debido a la ausencia de una regulación específica sobre contratos autoejecutables codificados en lenguaje informático. Esta falta de definición normativa ha generado un debate doctrinario respecto a su verdadera naturaleza: si constituyen “contratos” en los términos del Código Civil peruano o si deben considerarse únicamente como herramientas tecnológicas aplicables al comercio electrónico. En esta línea, Adolfo Morán advierte que existe discusión sobre si los smart contracts pueden calificarse jurídicamente como contratos o si deben entenderse simplemente como mecanismos de ejecución automática, similares a una transferencia bancaria utilizada para cumplir una obligación de pago²⁰.

Otro de los principales desafíos para la implementación efectiva de smart contracts en el Perú radica en su compatibilidad con las exigencias formales del Derecho civil, particularmente en lo concerniente a la escritura pública y la forma solemne exigida en ciertos actos jurídicos²¹. De acuerdo con el artículo 140 del Código Civil peruano, la observancia de la forma prescrita es requisito de validez para determinados contratos. En consecuencia, si bien los smart contracts podrían ser plenamente válidos en actos de naturaleza consensual o en operaciones contractuales privadas (como la preventiva de inmuebles sin transferencia inmediata de propiedad), no podrían sustituir los mecanismos notariales y registrales cuando la ley impone solemnidades, como sucede en la compraventa definitiva de bienes inmuebles y su solicitud de inscripción ante los Registros Públicos.

Frente a estas limitaciones, una posible vía de adecuación jurídica puede encontrarse en el desarrollo de marcos normativos flexibles (soft law) o reformas legislativas específicas que reconozcan la validez y eficacia de los smart contracts en determinados ámbitos. Experiencias comparadas, como el informe de la Law Commission del Reino Unido, sugieren que no siempre es necesario reformar profundamente el derecho privado

²⁰ Morán, El valor de la confianza, 312.

²¹ Por ejemplo, para acceder a los registros públicos, el contrato de compraventa debe ser elevado a escritura pública, de conformidad con el art. 2010 del Código Civil.

para admitir la operatividad de los smart contracts, sino que puede bastar con una interpretación funcional de la capacidad, objeto, la causa y la manifestación de voluntad.

En este contexto de progresiva digitalización contractual, el rol del notariado y de la SUNARP adquiere una especial relevancia. Lejos de quedar desplazados por la tecnología, estas instituciones deben participar activamente en el proceso de transición hacia sistemas jurídicos más digitales. El notariado, en particular, puede asumir una función de verificación y validación de los hitos contractuales ejecutados mediante smart contracts, aportando seguridad jurídica a los procesos automatizados y sirviendo como puente entre los entornos digitales y el ordenamiento legal tradicional.

Del mismo modo, la SUNARP podría incorporar herramientas tecnológicas que permitan la interoperabilidad con plataformas *blockchain*, facilitando la inscripción de actos contractuales originados digitalmente, siempre que se respete el principio de legalidad y se garantice la integridad de los datos. La desmaterialización del proceso contractual no implica la supresión de los controles formales, sino su adecuación a nuevas formas de manifestación de voluntad, soportadas por tecnologías confiables y auditables.

No puede dejar de mencionarse que, uno de los principales desafíos técnicos asociados a los smart contracts es el riesgo de codificación defectuosa. Dado que estos contratos se ejecutan automáticamente conforme al código programado, cualquier error lógico, ambigüedad²² o vacíos en su redacción puede producir consecuencias jurídicas no previstas ni deseadas. A diferencia de los contratos tradicionales —cuyas cláusulas pueden ser interpretadas bajo principios como la buena fe o el equilibrio contractual—, los smart contracts carecen de flexibilidad interpretativa, ejecutándose de manera estricta y literal. En consecuencia, resulta indispensable una colaboración interdisciplinaria entre

²² Como advierte Iryna Fetsyak, los smart contracts presentan retos propios del lenguaje informático, pues requieren que el objeto del contrato sea “cierto” y exento de ambigüedades, a diferencia del lenguaje natural. Asimismo, el pseudoanonimato que brinda la tecnología *blockchain* conlleva el riesgo de que se utilicen para fines ilícitos. Véase Iryna Fetsyak, “Contratos inteligentes: análisis jurídico desde el marco legal español,” *Revista Electrónica de Derecho de la Universidad de La Rioja* (REDUR), núm. 18 (2020): 217, citando a M. B. Aparicio Bijuesca y A. Savelyev.

programadores y juristas para asegurar que las condiciones contractuales queden correctamente plasmadas en lenguaje computacional, así como la inclusión de mecanismos de reversión o ajuste frente a fallos técnicos o abusos.

La implementación de la tecnología *blockchain* enfrenta obstáculos estructurales y regulatorios, pues requiere personal especializado, inversiones tecnológicas y una transformación gradual de los sistemas jurídicos y administrativos. Además, el carácter anónimo de algunas criptomonedas asociadas plantea riesgos de lavado de activos y financiamiento ilícito, generando preocupaciones de supervisión y cumplimiento. Esta falta de regulación clara genera un escenario de incertidumbre jurídica que, a su vez, limita el desarrollo y aplicación más amplia de soluciones basadas en *blockchain*, especialmente en entornos contractuales donde se requiere seguridad jurídica y trazabilidad²³.

La progresiva desmaterialización del derecho, especialmente en el ámbito de los derechos reales, ha generado un escenario en el que los objetos jurídicos dejan de ser necesariamente materiales para convertirse en representaciones simbólicas o digitales, manteniendo efectos jurídicos válidos. No obstante, como advierte Trazegnies, esta evolución no ha suprimido las exigencias formales que garantizan la seguridad jurídica²⁴, particularmente en el tráfico inmobiliario. En el Perú, pese a que los smart contracts podrían cumplir funciones como contratos preparatorios o herramientas operativas en la gestión contractual, no tienen aún la capacidad de generar efectos reales plenos por sí solos.

Consideramos que la transición hacia un sistema plenamente digital o automatizado requeriría una reforma estructural que reconozca legalmente estos nuevos instrumentos, sin renunciar a los principios de publicidad, autenticidad y seguridad jurídica que rigen actualmente el sistema registral.

Finalmente, la implementación de contratos inteligentes exige también abordar las brechas regulatorias y la necesidad de supervisión institucional. La falta de estándares técnicos, la ausencia de regulación

²³ Véase Corrales, Fenwick y Haapio, *Legal Tech, Smart Contracts and Blockchain*, 6.

²⁴ Véase Fernando de Trazegnies Granda, "La desmaterialización del Derecho," *Themis*, núm. 38 (2000): 11-12.

específica sobre oracles o plataformas autorizadas, y la inexistencia de mecanismos de certificación del código fuente, generan incertidumbre jurídica. En este escenario, el rol del Estado no debe ser el de obstaculizar la innovación, sino más bien establecer un marco de gobernanza tecnológica que permita el desarrollo responsable y seguro de herramientas digitales como los smart contracts, especialmente en sectores de alta sensibilidad como el inmobiliario.

VI. Conclusiones

La compraventa de inmuebles futuros en el Perú, si bien representa una opción económicamente atractiva para los compradores, continúa presentando elevados niveles de riesgo debido a la ausencia de garantías jurídicas efectivas especialmente en la etapa de preventa. Esta deficiencia ha dado lugar a prácticas contractuales abusivas, incumplimientos reiterados y una crisis de confianza en el mercado inmobiliario. La falta de mecanismos normativos que aseguren el uso exclusivo de los fondos entregados por los compradores para la ejecución del proyecto pone en evidencia la necesidad urgente de reformar el régimen de garantías aplicables a esta etapa.

Frente a este panorama, el ordenamiento jurídico peruano reconoce figuras contractuales tradicionales que podrían mitigar estos riesgos, tales como el fideicomiso en garantía, la cuenta escrow y el contrato de depósito en interés del depositario. No obstante, su implementación en la etapa de preventa ha sido limitada por factores como los altos costos de estructuración, la complejidad operativa o el desconocimiento de su aplicación. A pesar de estas limitaciones, su correcta utilización podría fortalecer la protección del comprador y garantizar un uso adecuado de los recursos captados, incrementando así la transparencia y previsibilidad en el desarrollo de los proyectos inmobiliarios.

En este contexto, los smart contracts y la blockchain se presentan como herramientas disruptivas que automatizan el cumplimiento de contratos de preventa, reducen el riesgo de incumplimiento y mejoran la trazabilidad de los fondos. Su aplicación en las etapas iniciales de la compraventa puede fortalecer la seguridad y eficiencia del proceso, especialmente si se complementa con garantías personales o cláusulas de penalidad codificadas.

Sin embargo, su implementación plena aún enfrenta desafíos normativos y técnicos. En el contexto peruano, la exigencia de solemnidades como

la escritura pública y la inscripción registral para la transmisión de derechos reales impide que los smart contracts generen efectos jurídicos reales sin cumplir con los requisitos formales establecidos por la ley.

Aello se suman la falta de regulación específica, los riesgos de codificación defectuosa y las limitaciones institucionales para supervisar estas tecnologías. Por tanto, se requiere una estrategia integral que combine reformas normativas, desarrollo de estándares técnicos y participación interinstitucional para viabilizar progresivamente su incorporación en el ecosistema contractual inmobiliario.

Los activos digitales y su tratamiento jurídico nacional desde la óptica del Derecho Privado

Martin Mayandía Burns* y Diego Augusto Munares Cutipa**

Resumen.– Este trabajo presenta un análisis comparado sobre la evolución normativa de los activos digitales, con énfasis en los tokens, y propone una aproximación jurídica desde el Derecho Privado peruano para abordar su tratamiento en el marco normativo nacional.

Palabras clave.– Activos digitales - Bienes incorpóreos - Derecho comparado - Derecho peruano - Regulación – Cadena de Bloques – Mercado de valores.

Abstract.– This paper presents a comparative analysis of the regulatory evolution of digital assets, with a focus on tokens, and proposes a legal approach from the perspective of Peruvian Private Law to address their treatment within the national legal framework.

Keywords.– Digital assets – Intangible goods – Comparative law – Peruvian law – Regulation – Blockchain – Capital markets.

* Socio en Petra Legal. LLM en Columbia University. MBA en Cornell University. Abogado en la Universidad de Lima.

** Asociado en Petra Legal. Becario ELAP en la Université de Montréal. Bachiller en Derecho por la Universidad Nacional Mayor de San Marcos.

I. Introducción

En la ópera magna de García Márquez¹, Melquiades le mostró a José Arcadio Buendía el funcionamiento de la alquimia, una práctica que aspiraba a la creación de oro a través de procesos químicos con tintes mágicos.

De igual manera, el profesor Francesco Galgano² sostiene que, en la era de las finanzas, el Derecho ha alcanzado el mismo objetivo que la alquimia mediante técnicas jurídicas capaces de generar riqueza a través de la estructuración de complejos productos financieros.

En ese sentido, la *lex mercatoria* formada por normas consuetudinarias orientadas a regular las relaciones comerciales establecidas en el mercado, sin tener en cuenta las políticas públicas, no tenía en cuenta que con el estado moderno estas normas consuetudinarias serían positivizadas en códigos comerciales.

En un contexto de globalización, Galgano advierte que la nueva *lex mercatoria* ha emergido orientada a consolidar los estándares contractuales y establecer una función jurisdiccional estándar a través del arbitraje. Estas funciones serían asumidas por organismos internacionales que recojan dichas prácticas comerciales en normas estatutarias, relegando al Estado a un rol adoptante.

Publicado en 1995, este diagnóstico exige una revisión crítica a la luz de la transformación del comercio global. Los contratos de derivados, ejemplo del antiguo proceso alquímico, han incorporado hoy una nueva “sustancia”: la tecnología.

Este artículo se propone explorar, con las herramientas jurídicas disponibles, los principales aspectos de los activos digitales en el ordenamiento nacional, y sostiene que estos no deben ser considerados como bienes muebles sin la existencia de un régimen jurídico específico que regule las relaciones patrimoniales sobre estos activos.

¹ MÁRQUEZ, G., *Cien años de soledad* (Buenos Aires: Editorial Sudamericana, 1967), pp. 45.

² GALGANO, F., “The New Lex Mercatoria,” *Annual Survey of International & Comparative Law* 2, no. 1 (1995), pp. 99-120, <https://digitalcommons.law.ggu.edu/annlsurvey/vol2/iss1/7/>.

II. Activos Digitales: Conceptos claves y características

En la presente sección realizaremos una revisión de las principales aproximaciones técnicas sobre el concepto de activo digital a fin de determinar sus principales características definitorias y el alcance del término.

Los activos digitales son aquellos que existen naturalmente en forma digital, y que pueden ser una representación de un activo real en dicho mundo digital, la mayoría de *criptoactivos* son activos digitales. Los *criptoactivos* son aquellos creados o facilitados por la tecnología *blockchain* garantizada a través del uso de la criptografía (Stabile et al, 2020)³.

La tecnología *blockchain* nos ha llevado a una nueva generación del internet que es denominada como *Web3*, esta última reinventa la forma como la información es almacenada y administrada en el internet proveyendo un único conjunto de información la cual es administrada por todos los nodos existentes en la red.

Este registro único permite la liquidación de operaciones en internet sin la necesidad de intermediarios, lo cual permite verdaderas transacciones *peer to peer* ("P2P"). Esta información es administrada colaborativamente por una red P2P de computadoras. Las reglas de administración son formalizadas en un protocolo y garantizadas por el consenso mayoritario de los participantes de la red, cuyas actividades son incentivadas con la emisión de *tokens* (Voshmgir, 2020)⁴.

El protocolo formaliza las reglas de gobernanza de la red y asegura que las personas que, en operaciones incógnitas donde la confianza entre pares escasea, se celebren transacciones. A diferencia de un sistema centralizado, donde la ciberseguridad se encuentra concentrada en un servidor central, el sistema de *Web3* desconcentra el riesgo de hackeo o ciberataques en diferentes nodos a través de la red.⁵

Por otro lado, los *smart contracts* pueden ser utilizados dentro de entidades o fuera de la red de *blockchain*. Los proveedores de data externa, también

³ STABILE, D. et al. (2020). Digital Assets and Blockchain Technology. U.S. Law and Regulation. Massachusetts: Edward Elgar Publishing.

⁴ VOSHMGIR, S. (2020). Token Economy: How the Web Reinvents the Internet. Vienna: Token Kitchen.

⁵ *Ibid.*, pp. 22.

llamados *oracles*, introducen información que es relevante para un *smart contract* desde fuera de la *blockchain*. Estos pueden efectuar la ejecución de un contrato en tiempo real y, por lo tanto, pueden reducir costos en el cumplimiento y la supervisión del contrato. Específicamente, se reducen los siguientes costos: (i) estructuración, (ii) formalización y (iii) vinculatoriedad.

El termino *smart contract* en sí mismo es desafortunado, debido a que no son particularmente inteligentes ni reflejan un reconocimiento legal. Este último solo puede ser considerado *smart* si las personas lo programan teniendo en cuenta toda la información disponible al momento de la programación. Asimismo, los *smart contracts* podrían tener cierto reconocimiento legal si cumple ciertas condiciones para lo cual se deben absolver ciertas incógnitas tecno-legales que demandan un diálogo interdisciplinario entre juristas y desarrolladores.

El proceso de *tokenización* de activos demanda la incorporación de todos estos sistemas para su eficiente funcionamiento en el cual desmaterializarán de manera descentralizada ciertos activos para que su circulación se realice a través de mecanismos tecnológicos sofisticados como la *blockchain*.

III. Revisión doctrinal y casuística sobre la naturaleza jurídica de los activos digitales

La presente sección tiene como finalidad realizar una revisión sobre las principales investigaciones jurídicas tanto a nivel nacional como internacional que versen sobre la naturaleza jurídica de los activos digitales.

A nivel nacional no tenemos una extensiva literatura jurídica que trate el tema, no obstante, hemos decidido tener presente las posiciones expuestas a continuación:

En primer lugar, Caveroy Legua (2020)⁶ sostiene que el sistema *blockchain* permite tener evidencia de la creación y/o procedencia de una obra o invención a partir de un registro confiable de los bienes intelectuales.

⁶ SAFRA, E., LEGUA, C. (2020). Un rincón en el archivo de tu corazón: Tecnología *blockchain* y privatización de activos digitales. *Revista de Actualidad Mercantil*, 6, pp. 172-187.

Por otro lado, Gutiérrez (2017)⁷ realiza una revisión de la naturaleza económica y jurídica del Bitcoin donde sostiene lo siguiente:

- a. El *Bitcoin* es un activo no financiero digital debido a que es, por lo menos, un depósito de valor para quien lo utiliza con intenciones especulativas y tiene un valor de cambio, o un valor de mercado, y por ello califica como un activo ya que reporta un valor a quien lo posee. Además, es un tipo de activo digital toda vez que opera mediante una computadora siempre que esta cuente con acceso a Internet.
- b. El Bitcoin es un bien incorporal que se rige por el tratamiento que el Código Civil dispone de los bienes muebles debido a que posee contenido patrimonial para quienes lo adquieren y porque tiene existencia autónoma.
- c. El Bitcoin es un bien incorporal con características funcionales propias que, por el momento, solo puede recibir el tratamiento que el Código Civil provee a los bienes muebles.

Ello porque no coincide con ninguno de los conceptos que dicho código define como bienes inmuebles lo que permite que este bien incorporal por ficción legal pueda ser considerado bien mueble.

Asimismo, desde la óptica internacional, García-Teruel y Simón Moreno⁸ concluyen que desde el derecho privado existe una tendencia a conceptualizar a los tokens como activos digitales, lo cual podría ser un punto de partida para una regulación de asset-backed tokens a nivel nacional. Sin embargo, desde el punto de vista de las normas de transferencia de propiedad es necesario que estas sean adaptadas para considerar a la tecnología *blockchain*.

Por otro lado, Lee⁹ señala que teniendo en cuenta que la propiedad ha sido la base fundamental para la construcción de estructuras económicas

⁷ GUTIÉRREZ, O., MORENO, A. (2017). El bitcoin: Consideraciones financieras y legales sobre su naturaleza y propuesta de enfoque para su regulación. Lima: Universidad ESAN.

⁸ GARCÍA-TERUEL, R., SIMÓN-MORENO, H. (2021). The Digital tokenization of property rights: A comparative perspective. *Computer Law & Security Review*, 41, pp. 1-16.

⁹ LEE, L. (2024). Examining the legal status of digital assets as property: A comparative analysis of jurisdictional approaches. arXiv, Cornell University.

y sociales, los activos digitales presentan desafíos en cuanto a la aplicación de las normas de propiedad por las teorías tradicionales que las fundamentan, este tipo de activos suelen intersecar con el concepto de propiedad intelectual, no obstante, la falta de claridad al determinar al creador o titular hace difícil su clasificación.

Adicionalmente, Rodríguez de las Heras¹⁰ señala que el *Digital Assets and Private Law Principles* son fuentes de *soft law* que servirán de referencia para la armonización de los cuerpos legales nacionales en cuanto se refieran a la ejecución y al tratamiento de los activos digitales desde el Derecho Privado.

Como se puede observar a nivel internacional existen diferentes investigaciones científicas sobre el tratamiento de los tokens, que se pueden incluir como una especie de activos digitales, en cuanto a su tratamiento desde el punto de vista del Derecho Privado, dichas posiciones jurídicas serán nuestro punto de partida para esbozar nuestra posición sobre el tratamiento de los activos digitales conforme al Derecho Privado en el ordenamiento jurídico nacional.

IV. El tratamiento de los activos digitales desde el Derecho comparado

El Derecho comparado se puede definir como un proceso en el que el comparatista toma varios objetos para estudiarlos dentro de un marco científico en el que un objeto o elemento estudiado se considera en función del otro. En este caso, estos objetos son el ordenamiento jurídico doméstico o nacional y el extranjero, el contraste entre estos dos objetos de estudio genera progresión del conocimiento.¹¹

¹⁰ DE LAS HERAS, T. The emergence of principles and best practices on digital assets: proprietary rights and enforcement. *European Journal of Risk Regulation*, 15, pp. 1-12.

¹¹ GEOFFREY, S. (2014). *An introduction to comparative law theory and method*. Oxford: Hart Publishing. Citado en: MUNARES, D. (2021). La función del derecho comparado en la unificación del Derecho Financiero latinoamericano: Breve demostración relacionada a la intermediación de valores. Ius360. Disponible en: <https://ius360.com/la-funcion-del-derecho-comparado-en-la-unificacion-del-derecho-financiero-latinoamericano-breve-demostracion-relacionada-a-la-intermediacion-de-valores-diego-munares/>

Esta mantiene como función principal el conocimiento del derecho, a pesar de como algunos pretenden restarle legitimidad señalando que este no mantiene ninguna aplicación práctica, el profesor de Turín, Rodolfo Sacco¹² señala que el derecho comparado no necesita de prestar justificaciones semejantes a la práctica. “La ciencia midió la distancia entre la tierra y la luna mucho antes que esta sea utilizada en la práctica”.

Gracias a la comparación el jurista percibe mejor lo que es original, lo que es constante, lo que resiste a los cambios, lo que es latente y lo que falta por explorar en su propio derecho, este permite conocer su propio ordenamiento jurídico apoyándose en otros.

En ese sentido, es menester recurrir a esta disciplina jurídica para explicar cómo se ha venido desplegando la regulación en otras tradiciones jurídicas, para lo cual exploraremos, dos (02) sistemas de las principales tradiciones jurídicas, por el lado del *common law*, exploraremos el derecho estadounidense; y, por el *civil law*, analizaremos el Derecho comunitario europeo haciendo especial énfasis en el Derecho español.

i. La regulación de los activos digitales en el common law

En el sistema estadounidense, teniendo en cuenta su sistema político federal, los activos digitales se han analizado desde la perspectiva de tres (3) reguladores federales: (i) la *Securities Exchange Commission*, (ii) *Commodity Futures Trading Commission* y (iii) *Financial Crimes Enforcement Networks*. De los cuales nos centraremos en el análisis elaborado por los dos (02) primeros.

A. Securities Exchange Commission

Desde la perspectiva de la *Securities Exchange Commission* (en adelante, “SEC”) la cual tiene como marco regulatorio a los denominados *securities*, los cuales son definidos como contratos de inversión con ciertas características que motivan la intervención

¹² SACCO, R. (1991). La comparaison juridique au service de la connaissance du droit. Aix-en-Provence: Presses Universitaires d'Aix-Marseille. Citado en: MUNARES, D. (2021). La función del derecho comparado en la unificación del Derecho Financiero latinoamericano: Breve demostración relacionada a la intermediación de valores. Ius360. Disponible en: <https://ius360.com/la-funcion-del-derecho-comparado-en-la-unificacion-del-derecho-financiero-latinoamericano-breve-demostracion-relacionada-a-la-intermediacion-de-valores-diego-munares/>

del Estado, en el Perú desde una perspectiva funcional, los valores mobiliarios serían el símil de la figura anglosajona antes mencionada.

En ese sentido, la SEC al ver la propalación del intercambio de los *tokens* digitales, el 3 de abril de 2019, publicó un documento denominado *Framework for 'Investment Contract' Analysis of Digital Assets* (2019)¹³, donde efectuó un ejercicio lógico de subsunción a fin de determinar si estos podrían calificar como *securities*, valiéndose del académicamente conocido *test* de *Howey*.

La prueba *Howey* se desprende del *leading case* denominado SEC v. W.J. Howey, mediante deducción jurídica se establece una regla general para calificar los *securities*, los cuales eran calificados como contratos de inversión que existían cuando había una inversión de dinero en una empresa común con una expectativa razonable de obtener beneficios derivado del esfuerzo de terceros.

De dicha premisa se desprendían los siguientes elementos configuradores: (i) Inversión de dinero, (ii) Empresa Común y (iii) Expectativa razonable de la obtención de beneficios del esfuerzo de terceros.

Con dicha disposición normativa, la SEC realizó una evaluación de estos activos de la siguiente manera:

- Inversión de dinero

El primer requisito del *test* de *Howey* generalmente se cumple en una oferta y venta de un activo digital, ya que el activo se compra o adquiere a cambio de un valor, ya sea en forma de dinero, *fiat money*, otro activo digital u otro tipo de contraprestación.

- Empresa común

Los tribunales norteamericanos han analizado este requisito como un elemento distinto al contrato de inversión. En la

¹³ U.S. Securities and Exchange Commission. (2019). Framework for "Investment Contract: Analysis of Digital Assets. Washington, D.C.: Securities and Exchange Commission.

práctica, los activos digitales usualmente conllevan a la existencia de una empresa común.

- Expectativa razonable de la obtención de beneficios del esfuerzo de terceros

Este requisito consiste cuando algún promotor, auspiciador o un tercero provee esfuerzos administrativos esenciales que impacten de manera directa en el éxito de la empresa, y que puede generar una expectativa de obtener beneficios económicos de estos.

Sobre este apartado, la SEC señala diferentes situaciones donde se cumplirían estos requisitos, normalmente son *tokens* que pueden otorgar el derecho a sus tenedores de percibir beneficios económicos, ya sea en dinero o en otros *tokens*, o que se puedan apreciar económicamente para obtener ganancias de capital en mercados secundarios.

B. Commodity Futures Trading Commission

Conforme a lo establecido en la *Commodity Exchange Act* establece que la definición de *commodity* incluye a los bienes, servicios, derechos, intereses sobre los cuales contratos de entrega futura pueden ser llevados a cabo en la actualidad o en el futuro.

La definición del cuerpo normativo anteriormente indicado, no solo se limita a los *commodities* tangibles, en ese sentido, dependerá mucho de la estructura de los *tokens* para ser considerados como *swaps*, *futures*, *options* u otros derivados financieros.

En ese sentido, la *Commodity Futures Trading Commission* ha determinado su competencia regulatoria en el caso de la existencia de activos digitales teniendo en cuenta los siguientes aspectos: (i) propósito funcional primario, (ii) no otorgamiento de derechos financieros, (iii) acceso a bienes o servicios, (iv) mercado secundario limitado, (v) emisión y oferta razonables y (vi) transparencia y divulgación.

ii. La regulación de los activos digitales en el derecho europeo

Los avances del Derecho europeo sobre el tratamiento de los *tokens* digitales lo conforman cuerpos normativos extensivos que exploran la naturaleza y el tratamiento de estos activos desde diferentes ópticas.

En ese sentido, en el año 2023, se promulgó el Reglamento (UE) 2023/1114 relativo al mercado de *criptoactivos* o también conocido como el Reglamento MiCA con la finalidad de desarrollar y promover la adopción de tecnologías transformadoras del sector financiero, incluida la adopción de la *Distributed Ledger Technology* (en adelante, “DLT”).

Dicho cuerpo normativo tiene las siguientes finalidades: (i) fomentar la innovación, (ii) evitar la fragmentación regulatoria, y (iii) proteger a los inversores.

Asimismo, dentro de la calificación de *criptoactivo* dependerá de las características concretas y derechos derivados del *criptoactivo* en cuestión, con independencia de la tecnología que la sustente.

A fin de poder determinar a ciencia cierta como se podría clasificar un *criptoactivo* como instrumento financiero, ESMA ha elaborado un documento denominado “*Guidelines on the conditions and criteria for the qualification of crypto-assets as financial instruments*” este tiene como objeto brindar las herramientas necesarias a los regulados para determinar cuándo un *criptoactivo* se encontrará regulado por MiCA y cuando por MiFID II, para ello, aparte de las valores negociables típicos que se pueden encontrar en el mercado, también establece las principales características que deberá ostentar un instrumento financiero bajo el DLT. Dentro de estos, tenemos los siguientes: (i) Derechos económicos, (ii) Finalidad de la emisión y (iii) existencia de obligaciones contractuales.

Asimismo, si observamos el devenir histórico de la circulación del crédito en el mercado de capitales, inicialmente estos circulaban a través de papeles timbrados y firmados por sus respectivos emisores después, debido al *paper crunch*, se creó la desmaterialización de dichos documentos que representaban valores mobiliarios a través de las anotaciones en cuenta en los Depósitos Centralizados de Valores. Ahora bien, de manera dialéctica consideramos que el siguiente paso de la evolución de la representación de valores mobiliarios es a través de la tecnología DLT, motivado por la crisis del año 2008 donde la confianza en las instituciones financieras fue altamente cuestionada, la revolución tecnológica y la globalización del mercado de capitales.

Precursora de estas ideas es el ordenamiento jurídico español que a través de una modificación en su Ley de Sociedades de Capital (artículos 23 y 407), la Ley de Instituciones de Inversión Colectiva (artículos 7,9 y

46) y en la Ley de Enjuiciamiento Civil (artículo 517) reconoce el nuevo régimen de representación de valores negociables en la tecnología DLT.

Finalmente, en el año 2023 *International Institute for the Unification of Private Law* (UNIDROIT) publicó los *Unidroit Principles On Digital Assets And Private Law* donde a través del *soft law* se pretende establecer lineamientos para estructurar un marco legal coherente y predecible para las transacciones que involucren activos digitales.

iii. Regulación de los activos digitales en el Perú

En el Derecho Positivo peruano nos encontramos con regulación referente a la prevención del Lavado de Activos y Financiamiento del Terrorismo también conocido por sus siglas LA/FT.

El 30 de julio de 2024, mediante la Resolución SBS 02648-2024, se aprobó la Norma para la Prevención del Lavado de Activos y del Financiamiento del Terrorismo aplicable a los Proveedores de Servicios de Activos Virtuales (PSAV) bajo la supervisión de la UIF – Perú, donde a través del inciso 1) del artículo 3° de la norma de PSAV se define a los Activos Virtuales como *representaciones digitales de valor que se pueden comercializar o transferir digitalmente y se pueden utilizar para pagos o inversiones. No incluyen representaciones digitales de moneda fiat o de valores emitidos por el Banco Central o la autoridad competente de la jurisdicción.*

Por otro lado, a través de la Cuarta Disposición Complementaria del Decreto de Urgencia 013 – 2020, se modificó la Ley 30050 Ley de Promoción del Mercado de Valores estableciendo sobre la base del principio de primacía de la realidad la capacidad de poder regular determinados activos digitales que cumplan con la característica de ser un activo financiero.

A pesar de ello, la Superintendencia del Mercado de Valores a través de un comunicado oficial¹⁴ indica que al no existir regulación específica sobre las criptomonedas, monedas virtuales o *tokens* no ejercen supervisión sobre este segmento del mercado.

¹⁴ El Peruano. (2024). Criptomonedas en Perú: SMV alerta sobre fraudes y estafas en ofertas sin regulación. Consultado el 10 de abril de 2024. Disponible en: <https://www.elperuano.pe/noticia/265609-criptomonedas-en-peru-smv-alerta-sobre-fraudes-y-estafas-en-ofertas-sin-regulacion>.

Como podemos observar, la regulación de activos digitales en el Perú ha surgido de manera reactiva debido a recomendaciones internacionales como en el caso de la norma PSAV que fue impulsada por iniciativa de GAFI o por situaciones coyunturales ante el aumento de fraudes financieros a través de la utilización de este tipo de activos más no se ha generado una agenda regulatoria clara sobre este tipo de activos que van aumentando la profundidad de su mercado.

V. Fundamentación de la naturaleza jurídica de los Activos Digitales

Después de realizar una revisión en la legislación comparada de los principales sistemas jurídicos relacionados a dos largas tradiciones jurídicas¹⁵, es menester analizar cuál es el tratamiento de los activos digitales en el marco del esquema normativo peruano.

Somos de la posición de que, partir de un ejercicio de subsunción se debe determinar si estos pueden calificarse como objeto de derecho¹⁶, el cual, desde la definición ampliamente adoptada por la judicatura así como el sector doctrinario que esboza ciertas directrices al contenido de las instituciones jurídicas, nos debemos preguntar si los activos digitales son pasibles de ser un centro de imputación de deberes y derechos.

Para lo cual, debemos explorar en el extenso universo de instituciones jurídicas que positiviza nuestro sistema jurídico, si alguna de estas la recoge en el seno de su definición, ha habido aproximaciones e incluso interpretaciones por parte de ciertos órganos administrativos registrales que han realizado el análisis de si estos activos pueden considerarse como bienes muebles.

Para ello, nuestro Derecho común, específicamente en el apartado que regulan los derechos reales, ha efectuado la *summa divisio* entre bienes

¹⁵ GLENN, P. (2014). *Legal Traditions of the World: Sustainable Diversity in Law*. Oxford University Press (5ta Edición).

¹⁶ CARNELUTTI, F., *Teoría General del Derecho* (Lima: Ara Editores, 2006), pp. 41. El autor sostiene que el objeto jurídico es aquello que se observa del Derecho, en tanto refleja el concepto que se tiene del mismo. Para ilustrarlo, propone una figura triangular cuyos vértices representan a las partes y a la cosa, elementos esenciales de toda relación jurídica.

muebles e inmuebles, contando la primera categoría con una amplia dispersión por una cláusula *numerus apertus* mientras que la segunda con un *numerus clausus*.

En ese sentido, dentro de la división establecida, *in prima facie*, se podría desprender que los activos digitales pueden ser calificados como bienes muebles, no obstante, debemos dar un paso atrás y analizar si estos pueden calificar bajo la calificación de Bien.

En ese sentido, consideramos que el concepto jurídico de bien o cosa, es cualquier entidad, material o inmaterial, que sea jurídicamente relevante, esto es, que sea tomada en consideración por la ley, en cuanto constituye o puede constituir relaciones jurídicas.¹⁷

Asimismo, cierto sector de la doctrina comparada distingue que los bienes pueden tener dos acepciones; una amplia, donde el bien es igual a las cosas (objetos materiales) como los objetos inmateriales susceptibles de valor que serían los derechos y, por otro lado, una restringida que equipara a los bienes a exclusivamente objetos incorpóreos.¹⁸

Dicha distinción históricamente proviene de un pasaje de las *Institutas de Gayo*, donde se expresa de manera taxativa que las cosas se dividen en bienes corporales e incorpóreos. Los primeros referidos a cosas tangibles mientras que los segundos a cosas intangibles como las que constituyen un derecho como la herencia, el usufructo, o las obligaciones de cualquier modo se hayan contraído.¹⁹

Nuestro ordenamiento jurídico adopta la acepción amplia de bien donde engloba a los bienes corporales e incorpóreos que pueden ser objeto de derecho, no obstante, no todo objeto de derecho es calificado como un bien.

En esa misma línea, el doctrinario italiano, Biondo Biondi²⁰, esboza de manera profunda y detallada, las principales características de los bienes muebles:

¹⁷ BIEONDI, B. (1953). I beni. Milano: Dott. A. Giuffrè.

¹⁸ MARIANI, M., ABELLA, A. (2016). Derechos Reales. Buenos Aires: Zavalía.

¹⁹ *Ibid.*, pp. 50

²⁰ BIONDI, op. cit., pp. 42.

- a) Extrañeza de sujeto.
- b) Relevancia jurídica.
- c) Individualización en el mundo externo.
- d) Independiente.
- e) No se requiere actualidad de la cosa
- f) Utilidad o potencial utilidad.
- g) Aislamiento.

Ahora bien, consideramos que es necesario establecer una primera aproximación de los activos digitales desde la clasificación de bienes corporales e incorporeales, la cual proviene desde el Derecho romano avocada a lo que, por un lado, Cicerón determinó como aquellas cosas que se pueden poseer y se representan por una entidad material; y, por el otro lado, aquellas que la voluntad puede poseer, como la usucapión, tutela y la *gens*.²¹

Asimismo, la doctrina nacional identifica, analizando el artículo 886 del Código Civil, los tipos de bienes muebles reconocidos por el legislador, los cuales se pueden dividir en: (i) muebles por naturaleza, (ii) muebles por analogía, y (iii) muebles por ficción legal. Estos últimos son aquellos que son imperceptibles por los sentidos, y sobre los cuales no puede predicarse su condición de movilidad o inmovilidad.²²

Sobre los bienes incorporeales no son abarcados bajo el tratamiento de los derechos reales debido a que no se adecúan a perfectamente al régimen debido a que no existe posesión, usucapión ni tradición, tratamiento similar al adoptado por Código Civil Alemán (BGB)²³

Por lo tanto, los factores diferenciales que alejan el régimen jurídico de bienes corporales e incorporeales son esencialmente dos, el hecho generador de atribución y la determinación de los bienes.

En primer lugar, el hecho generador de atribución de los bienes corporales se caracteriza por ser posesoria mientras que en los bienes incorporeales esta característica es distinta. Como señala Mario Rotondi, los objetos

²¹ *Ibid.*, pp. 13

²² GONZÁLES, G. (2019). Tratado de derechos reales. Lima: Jurista Editores.

²³ MARIANI Y ABELLA, op. cit., pp. 55.

incorporales se convierten en bienes cuando tiene contenido patrimonial y son susceptibles de tutela jurídica autónoma.²⁴

En segundo lugar, los bienes corporales conforman una categoría indefinida pues no existen límites para la apropiación de las realidades del mundo externo, siempre que consistan en entidades físicamente sometibles a la voluntad del titular y valorables económicamente, mientras que los bienes incorporales, su tutela se halla limitada a las modalidades previstas en la ley.²⁵

No obstante, en nuestro ordenamiento jurídico, la cuestión de bienes incorporales no está cerca de resolverse, entendiendo a los bienes como aquellos que pueden ser objeto de derecho, qué duda cabe los bienes corporales si pueden enmarcarse en el tratamiento expreso del Código Civil, mientras que los incorporales resultan precisamente relevantes dependiendo del tratamiento jurídico que se establezca más que cualquier consideración doctrinaria.²⁶

En ese sentido, conforme a lo indicado en la primera sección del presente trabajo, existen posiciones doctrinarias que consideran a los activos digitales como bienes muebles incorporales fundamentando su posición en el *numerus apertus* de los bienes muebles e indicando que específicamente un tipo de activo digital como el *bitcoin* califica como bien mueble al tener contenido patrimonial y al gozar de autonomía.

Desde nuestra perspectiva jurídica sostenemos la posición de que los activos digitales no son bienes muebles pasibles de derechos reales debido a que a pesar de las posiciones doctrinarias e interpretativas subsumiendo estos instrumentos en un *numerus apertus*, estos necesitan de un cuerpo normativo específico que establezcan prerrogativas adaptables a la funcionalidad de los activos digitales.

Ahora bien, valiéndonos de las posiciones doctrinarias anteriormente citadas encontramos que los activos digitales no son bienes muebles debido a que estos carecen de relevancia jurídica al no ser regulados por una norma de carácter especial indicando que estos pueden ser pasibles de relaciones jurídicas (objeto de derecho). El *numerus apertus* de los

²⁴ GONZÁLES, op. cit., pp. 240.

²⁵ *Ibid.*, pp. 240.

²⁶ BIONDI, op. cit., pp. 58.

bienes muebles establecido en el Código Civil se encuentra enfocado en abarcar la totalidad de bienes muebles corporales que no pueden ser enunciados por su extensa pluralidad e históricamente los bienes incorporeales han sido definidos como derechos subjetivos sobre los cuales podría recaer voluntad de posesión, en consecuencia, ha sido una característica preexistente la existencia jurídica de estos.

Caso contrario, la libre determinación doctrinaria y valerse del *numerus apertus* de los bienes muebles, solamente omite un paso previo del análisis de calificar a los activos digitales como bienes que consecuentemente lo calificaría como objeto de derechos, por ende, genera el incentivo perverso de establecer relaciones espurias sobre idealidades y vivir en el mercado de las ideas haciendo un parangón al mundo que Platón esbozo en sus Diálogos.

Ahora bien, valiéndonos de la economía mediante el Análisis Económico del Derecho (en adelante, “AED”), también concluimos que los activos digitales en el ordenamiento jurídico peruano no deben considerarse como un bien mueble.

En ese sentido, la regulación específica de los activos digitales puede reducir los altos costos de transacción propios de este tipo de activos, esto a través de un régimen específico de propiedad que se adecúe a la naturaleza de este tipo de activos.

En ese sentido, Ronald Coase²⁷ indica que el problema de las externalidades, lo que es un fundamento base para el costo social, es solucionado por un sistema claro de derechos de propiedad.

En esa misma línea, el profesor de la Universidad de Chicago sostiene que las instituciones legales y económicas son relevantes y tienen impacto en el mercado debido a que los costos de transacción no son cero y además el derecho de propiedad no se encuentra perfectamente definido.

Ahora bien, en el mundo de los activos digitales los costos de transacción son altísimos debido a los siguientes factores: (i) alta asimetría de información, (iii) ambigüedad normativa, (iv) costos de resolución de conflictos.

²⁷ COASE, R. (1960). The problem of social cost. Journal of Law and Economics, 3, pp. 1-44.

Evidentemente los activos digitales como los *tokens* representan un alto grado de asimetría de información debido a que estos involucran el conocimiento de la tecnología *blockchain*, el protocolo de los *tokens*, las limitaciones tecnológicas y el código de contrato inteligente, sobre todo en los *security tokens* que involucran una inversión para ello la necesidad de una regulación específica que establezca medidas de revelación de información esencial en favor de la contraparte es indispensable para la reducción de los costos generados por esta falla de mercado.

Asimismo, en cuanto a la ambigüedad normativa esta se genera debido a que no existen disposiciones normativas claras que establezcan la naturaleza jurídica de este tipo de activos, en consecuencia, estos últimos no se podrían subsumir bajo un régimen legal para las transacciones realizadas, aunque a pesar de que como la línea académica y profesional jurídica indique que estos deberían ser calificados como bienes muebles, las disposiciones normativas no se adaptarían a las características de estos activos, lo cual tendría como consecuencia inmediata su ineficacia sobre este tipo de activos y una falsa percepción de seguridad jurídica.

En consecuencia, a pesar de que los activos digitales, específicamente los *tokens*, puedan ser calificados como bienes muebles no soluciona el problema sino lo agudiza al aumentar el riesgo de selección adversa al subsumir en el régimen de derechos reales bienes incorpóreales que no tienen una regulación específica cuyas disposiciones se adecúen a las características de este tipo de activos.

Ahora bien, analicemos un reciente pronunciamiento del Tribunal Registral de SUNARP²⁸ que analiza la naturaleza de un criptoactivo en el marco de la constitución de una sociedad.

El 13 de noviembre de 2024, el Tribunal Registral declaró fundada la apelación sobre la inscripción de la constitución de una sociedad anónima cerrada con criptomonedas como capital social y ordenó que esta se inscriba en el Registro de Personas Jurídicas, la cuestión a determinar en esta resolución fue si las criptomonedas pueden ser objeto de capital social en la constitución de la sociedad.

²⁸ Superintendencia Nacional de los Registros Públicos. (2024). Resolución 4920-2024-SUNARP-TR (NSIR-T). Tribunal Registral. Disponible en: <https://resolucion.tribunal.sunarp.gob.pe/sir-tribunal-publico/>

Ante ello, el Tribunal Registral realiza un análisis de subsunción jurídica inconexo enmarcando a las criptomonedas como bienes muebles, en primer lugar, define las características de un bien según Biondo Biondi, después esboza la clasificación de bienes materiales e inmateriales y, finalmente, termina con la siguiente *ratio decidendi*: “si bien las criptomonedas no tienen regulación legal especial, por ser una figura nueva que nace con los avances tecnológicos; no es menos cierto que, éstas encajarían dentro del supuesto establecido en el inciso 10 del artículo 886 del Código Civil [Cláusula abierta], por lo que serían consideradas como bienes muebles”.

El análisis del Tribunal Registral, desde nuestra perspectiva no sería el adecuado debido a que si bien enuncia las instituciones jurídicas que serían aplicables a fin de determinar la materia en cuestión no realiza el análisis de subsunción sobre este último. Haciendo un símil explicativo con el método científico es como exponer la metodología que se planea usar para demostrar una hipótesis, pero esta no se utiliza al momento de la comprobación.

El Tribunal Registral para determinar si efectivamente las criptomonedas son pasibles de utilizarse como capital de una sociedad anónima cerrada, debió realizar un análisis teniendo en cuenta lo siguiente de manera progresiva: (i) si las criptomonedas son bienes y (ii) que tipo de bienes son las criptomonedas.

Dentro de la parte considerativa del Tribunal Registral, uno de los criterios que otorga contenido a si algo debe ser considerado como bien es que este debe tener relevancia jurídica, lo que es indiferente al ordenamiento legal no es bien. La relevancia jurídica, es decir el interés, la impone la ley.

En ese sentido, retomamos lo que indicamos en párrafos precedentes, un tema es el análisis de la realidad desde el mundo ontológico, estableciendo la esencia de las criptoactivos, y otro diferente es el mundo jurídico que determina si efectivamente este tiene alguna consecuencia jurídica, por lo tanto, desde nuestro sistema positivista, no queda duda que los criptoactivos aún no gozan de efectos jurídicos al no tener un tratamiento específico.

Tomando como referencia a la propiedad intelectual, ya sean los derechos de autor o la propiedad industrial, estos bienes incorporeales para ser considerados así tienen un acogimiento expreso por parte del Código

Civil. Asimismo, ostentan de un tratamiento jurídico sofisticado a través de distintas fuentes normativas formales, lo mismo debería suceder con el tratamiento de los criptoactivos teniendo que ser reconocidos como bienes muebles de manera expresa y tener un tratamiento jurídico específico bajo fuentes formales de derecho.

VI. Conclusiones

Desde la perspectiva del Derecho Privado peruano podemos concluir lo siguiente:

- Los activos digitales no son bienes muebles debido a que al ser incorpóreos necesitan un cuerpo normativo específico que los haga pasibles de ser objeto de relaciones jurídicas.
- El otorgarle la naturaleza jurídica de bienes muebles a los activos digitales incrementará el riesgo de selección adversa por la generación de una falsa percepción de seguridad jurídica.
- Los activos digitales no pueden calificarse per se cómo valores mobiliarios bajo la supervisión de la SMV, es necesario que a través del principio de primacía de la realidad puedan subsumirse como un valor mobiliario positivizado en un cuerpo normativo específico.

Datos sintéticos y publicidad, desafíos legales en el uso de inteligencia artificial en campañas publicitarias

Malena Cárdenas Tello*

Resumen.- El artículo analiza los principales retos legales vinculados al uso de datos sintéticos desde la protección de datos personales, el principio de veracidad en la publicidad y su uso con el objetivo de simular un testeo publicitario en “consumidores” antes de que la campaña sea lanzada al mercado. Se revisarán sus implicancias legales, así como la regulación sobre esta materia a nivel mundial. Finalmente se abordarán las principales ventajas y desventajas que enfrentaría su uso.

Palabras clave.- Datos sintéticos - Campañas Publicitarias - Principio de Veracidad.

Abstract.- The article analyzes the main legal challenges associated with the use of synthetic data, focusing on personal data protection, the principle of truthfulness in advertising, and the use of such data to simulate advertising testing on “consumers” prior to the public launch of a campaign. The article analyzes its legal implications, as well as the emerging international regulatory approaches to this issue. It also discusses that mail advantages and potential drawbacks of its implementation.

Keywords.- Synthetic Data - Advertising Campaigns - Principle of Truthfulness.

* Magíster en Propiedad Intelectual e Industrial por la Universidad de Alicante, España. Abogada por la Universidad de San Martín de Porres. Actualmente se desempeña como Corporate Legal Counsel en BELCORP. Las opiniones vertidas en este artículo son de exclusiva responsabilidad de la autora y no representan la posición de la empresa en la que labora.

I. Introducción

En un contexto donde la inmediatez en obtener resultados es cada vez más apreciada por el consumidor, las empresas tienen el desafío de aprovechar al máximo el tiempo entre el desarrollo de productos o servicios de alta calidad y comunicar las bondades que ofrecen con campañas publicitarias atractivas y que logren conectar con el público.

Así, el uso de inteligencia artificial se ha convertido en una herramienta cada vez más potente para lograr estos objetivos, aplicándola en diversas etapas del proceso de desarrollo de productos y servicios.

Especial atención empieza a cobrar en el campo de la publicidad, específicamente en el desarrollo de campañas publicitarias, en donde con el objetivo de optimizar tiempos se empiezan a utilizar distintos recursos, entre ellos podemos encontrar a los datos sintéticos, aquellos datos creados utilizando inteligencia artificial, para mejorar el proceso de validación del mensaje que se quiere comunicar al público, reduciendo significativamente el tiempo y costo que ello implicaría, sobre todo cuando el anunciante tiene más de una opción de ruta a seguir.

En este escenario se propone crear grupos de perfiles sintéticos creados con inteligencia artificial, diseñados específicamente para simular el comportamiento de consumidores reales. Para lo cual, en lugar de testear la mejor ruta publicitaria a seguir para el lanzamiento de una campaña publicitaria frente a un grupo de 400 consumidores, el uso de datos sintéticos generados con inteligencia artificial podría generar 400 “consumidores sintéticos” tomando en consideración distintos patrones como género, edad, intereses de consumo y reacciones emocionales.

Actualmente algunas empresas de investigación de mercado y comportamiento del consumidor ofrecen los servicios de obtención de resultados de análisis del usuario sobre la base de datos sintéticos. Sin embargo, su uso, aun cuando a primera impresión puede parecer una opción bastante favorable, no está exento de desafíos desde el punto de vista jurídico.

Conforme desarrollaremos en el presente artículo, es importante considerar las implicancias legales en especial desde el frente de la privacidad y sesgos, a fin de que su uso sea seguro y el adecuado cumplimiento de regulaciones como el Reglamento General de Protec-

ción de Datos (GDPR) y la implementación de políticas internas con el fin de garantizar la correcta anonimización y trazabilidad de los datos.

II. Concepto de Datos Sintéticos

Los datos sintéticos son datos artificiales que se generan utilizando un modelo especialmente diseñado, por ejemplo, modelos de aprendizaje automático (ML, por sus siglas en inglés *machine learning*), los cuales se pueden obtener entrenando un modelo con un conjunto de datos personales reales de origen, de modo que puedan imitar las características, patrones y estructura de los datos personales originales. Como resultado, el análisis de datos sintéticos puede producir resultados similares a los obtenidos con los datos de origen (Personal Data Protection Commission Singapore, 2024)¹.

Si bien el concepto de datos sintéticos puede ser muy técnico, para efectos del presente artículo nos referiremos únicamente a los datos sintéticos utilizados para entrenar un modelo con perfiles de preferencias de consumidores.

Así, este uso de datos sintéticos se les conoce como datos sintéticos tabulares debido al formato que se usa, los cuales deben ser consistentes con las estadísticas recogidas de usuarios reales, a fin de entrenar modelos de análisis de comportamientos.

Para ahondar en el tema de los datos sintéticos tabulares, se refieren a los datos generados artificialmente para replicar la distribución de un conjunto de datos reales y producir muestras sintéticas de alta fidelidad, a la vez que logren preservar la privacidad².

Además, en la medida que la data usada no es real, estos datos encajan dentro de tipo de dato totalmente sintético.

Actualmente, los datos sintéticos han despertado mayor interés en distintos sectores industriales debido a que son considerados como un tipo de tecnología de mejora de la privacidad (PET, por sus siglas

¹ Personal Data Protection Commission Singapore (2024). Proposed guide synthetic data generation <https://www.pdpc.gov.sg/-/media/files/pdpc/pdf-files/other-guides/proposed-guide-on-synthetic-data-generation.pdf>

² SHI, R., WANG, Y., DU, M., SHEN, X., & WANG, X. (2025). A comprehensive survey of synthetic tabular data generation. arXiv.org. <https://arxiv.org/abs/2504.16506>.

en inglés *Privacy Technology*), en específico dentro de la categoría de ofuscación de datos, según la Organización para la Cooperación y el Desarrollo Económico (OCDE, 2023)³, de esta forma es posible tratar y analizar información para entrenar a la inteligencia artificial sin revelar los datos personales utilizados para el entrenamiento y con ello lograr una ventaja competitiva frente a otros competidores.

A diferencia de los métodos más clásicos de PET, como por ejemplo la técnica de anonimización de datos existe el riesgo de que los datos personales sean revelados aprovechando alguna brecha de seguridad, con los datos sintéticos se eliminaría este problema de raíz⁴ ya que los datos personales para entrenar al ML no serán compartidos.

III. Regulación comparada de los datos sintéticos

Hasta el momento el Perú no cuenta con ninguna norma que regule expresamente el uso de datos sintéticos, a diferencia de otras jurisdicciones como se desarrollará en el presente apartado; no obstante, se debe tener presente que cuando los datos sintéticos son creados a partir del uso de una base de datos personales, su tratamiento sí deberá cumplir con la Ley de Protección de Datos Personales⁵, así como su Reglamento⁶, puesto que en el referido escenario, los datos personales pasarán por un proceso de anonimización.

En contraste con el escenario que se presenta en Perú, la tendencia, en los últimos años, a nivel global ha sido que las autoridades competentes consideran necesario pronunciarse sobre el uso de los datos sintéticos, mediante la emisión de lineamientos para su uso de forma segura. A continuación, citaremos algunos casos a modo de ejemplo:

³ Organización para la Cooperación y el Desarrollo Económicos (OCDE). (2023). *Emerging privacy enhancing technologies: Current regulatory and policy approaches*.

⁴ Se indica “eliminaría” en condicional, debido a que más adelante profundizaremos sobre los posibles riesgos que implica el mal diseño de datos sintéticos.

⁵ Ley de Protección de Datos Personales, Ley N. 29733. Publicada el 3 de julio de 2011 en el Diario Oficial El Peruano.

⁶ Decreto Supremo 016-2024-JUS, que aprueba el Reglamento de la Ley N. 29733, Ley de Protección de Datos Personales.

Guía sobre la Generación de Datos Sintéticos – PDPC Singapur

- Esta guía desarrolla ampliamente el concepto de datos sintéticos, entendiéndolos como aquellos generados mediante modelos matemáticos que incluya el uso de inteligencia artificial, además precisa que existen tipos de datos sintéticos, enfocándose principalmente en aquellos datos completamente sintéticos, que se general sin usar data real, lo cual difiere de los datos parcialmente sintéticos, que combinar datos reales con generados.

También profundiza acerca de sus beneficios y principales riesgos, como sería el riesgo de reidentificar los datos de origen utilizados para generar datos sintéticos, para lo cual se deberán emplear técnicas como la adición de ruido o reducción de granularidad a fin de mitigar riesgos de reidentificación.

La guía emite además una serie de buenas prácticas para que las empresas que los empleen reduzcan los riesgos de seguridad, mediante la implementación de medidas técnicas y control de gobernanza del riesgo. Finalmente, brinda ejemplos de métodos de generación de datos sintéticos⁷.

Guía sobre IA y Protección de Datos- ICO UK

- En este documento se desarrolla el uso, en general, de inteligencia artificial en relación con los principios que deben cumplirse al procesar datos personales.
- La guía reconoce la existencia de los datos sintéticos como un mecanismo para mejorar la privacidad de los datos utilizados como fuente de entrenamiento de sistemas que emplean inteligencia artificial, los cuales a su vez generan datos sintéticos.
- Así, en caso las empresas utilicen datos sintéticos tiene el deber de documentar y auditar todo el proceso de generación y uso de datos con el fin de que puedan demostrar que garantizan la protección de los datos originales empleados como entrenamiento.

⁷ Personal Data Protection Commission. (2024). Proposed Guide on Synthetic Data Generation. <https://www.pdpc.gov.sg/help-and-resources/2024/07/proposed-guide-on-synthetic-data-generation>

Un punto no menor, es que las empresas que emplean los datos sintéticos también tienen el deber los modelos empleados, a fin de que eviten sesgos discriminatorios o resultados inexactos.

También refuerza la idea que, si los datos sintéticos no permiten identificar a personas específicas, no se considerarán datos personales y, por ende, las obligaciones de protección de datos no le aplicarán.

No obstante, en caso sí se lograra inferir información sobre aquellos datos personales originales a partir de los datos sintéticos, entonces sí deberán cumplir con las leyes de protección de datos⁸.

IV. Uso de los datos sintéticos en el lanzamiento de campañas publicitarias

No es novedoso señalar que una de las áreas en donde más se emplean herramientas entrenadas con inteligencia artificial es el marketing, ello ya que estas herramientas permiten analizar grandes volúmenes de data y personalizar mensajes publicitarios de manera mucho más exacta y rápida, frente a los métodos tradicionales.

De hecho, es común encontrar tanto empresas transnacionales como pequeños creadores de contenido en distintas redes sociales que emplean herramientas accesibles al público en general, logrando mejorar el alcance de su publicidad y comunicaciones o ajustando su estrategia en tiempo real según la respuesta que obtengas de la audiencia.

Sin embargo, poco se habla de que algunas empresas están empezando a incorporar dentro de sus procesos de testeo de rutas para el lanzamiento de campañas publicitarias herramientas más sofisticadas de evaluación, no tan difundidas, como por ejemplo aquellas que utilizan datos sintéticos.

Este tipo de herramienta permite que la empresa que la emplea pueda prever distintos escenarios de comportamiento de sus consumidores antes de que se implemente en la realidad, lo cual le generará un evidente

⁸ Information Commissioner's Office. (2023). Guidance on AI and Data Protection. <https://ico.org.uk/media2/ga4lfb5d/guidance-on-ai-and-data-protection-all-2-0-38.pdf>

beneficio en cuanto a la reducción de costos y en especial a riesgos de no obtener los resultados esperados si es que acaso se prescindiera de esta evaluación.

A efectos del presente artículo, es importante precisar que cuando mencionamos testeo de rutas, nos referimos únicamente al uso de datos sintéticos en la etapa de validación del mensaje publicitario y no respecto al testeo de los beneficios o de seguridad por el que debe pasar un producto antes de ser lanzado al mercado para no incurrir en infracciones de las normativas regulatorias, publicitarias y de protección al consumidor.

De esta forma, los datos sintéticos se generan sobre la base de datos personales como pueden ser ubicaciones demográficas y tendencias de comportamiento, los cuales son recopilados de una muestra representativa del público consumidor al que destinará su producto o servicio. Con ello, mediante el entrenamiento de la inteligencia artificial, es posible obtener una cantidad representativa y significativa de datos sintéticos, los cuales permitirán probar cada una de las rutas publicitarias propuestas y predecir el comportamiento del público objetivo.

El uso de datos sintéticos ha generado un creciente entusiasmo, ya que al ser generados de forma artificial permiten ampliar significativamente la cantidad de datos personales que se necesitan tratar y procesar con el fin de agilizar el proceso de testeo, sin tener que enfrentar las limitaciones o riesgos que, algunas veces, puede presentar el tratamiento de datos personales, en especial cuando se trata de vulneración a la seguridad de la información.

Los datos sintéticos también permiten explorar escenarios que, de usarse con datos personales, podrían resultar costosos y difíciles de evaluar. Por ejemplo, se podría usar datos sintéticos para probar distintas comunicaciones de un mismo mensaje o respecto a 3 rutas distintas en el diseño del empaque del producto, en un tiempo bastante acotado.

En definitiva, esta forma de utilizar los datos sintéticos permite recrear una suerte de audiencia sintética, la cual, mediante el procesamiento de distintas variables como lo son el historial de compras, el consumo de medios y análisis de sentimiento u otros comportamientos digitales, permite crear perfiles sintéticos que se comportan como consumidores

reales y permite obtener pronósticos precisos sobre la preferencia del público objetivo⁹.

Dentro de las principales ventajas que ha traído a la industria del marketing este tipo de uso de datos sintéticos, encontramos que se puede ver reducido significativamente el tiempo que toma experimentar distintos escenarios de comportamiento de los consumidores, al realizar una investigación de mercado sustituyendo las respuestas humanas con modelos predictivos o quizá utilizar panelistas humanos únicamente para las preguntas claves y complementar dicha información con muestras sintéticas obteniendo con ello resultados representativos. (Kalidas & Ostler, 2023¹⁰).

Sin perjuicio de ello, se debe considerar que existen ciertas limitaciones inherentes a su uso, ya que los datos sintéticos podrían reflejar sesgos presentes en los datos originales que se utilizan de entrenamiento. Por ello, se recomienda que la data obtenida de forma sintética sea utilizada de forma complementaria, incluso de requerirlo, haciendo una validación de los resultados con seres humanos para comparar el nivel de exactitud en las respuestas y así asegurar que la data obtenida sea confiable. (Kalidas & Ostler, 2023¹¹).

De hecho, de un estudio realizado por Qualtrics en donde se encuestaron a 3 000 investigadores de mercado de 14 países, se obtuvieron los siguientes resultados: 87% de aquellos encuestados que han utilizado respuestas sintéticas obtuvieron una alta satisfacción con los resultados arrojados. Además, un 71% de los encuestados coincide en que, dentro de tres años, la mayoría de la investigación de mercado se realizará utilizando respuestas sintéticas.

⁹ BRITO, M. Synthetic data: A new frontier in data-driven innovation. <https://www.britopian.com/research/synthetic-data/>

¹⁰ KALIDAS, A., & OSTLER, J. (2023). What is synthetic sample- and is it all it's cracked up to be? Kantar. <https://www.kantar.com/inspiration/analytics/what-is-synthetic-sample-and-is-it-all-its-cracked-up-to-be>

¹¹ KALIDAS, A., & OSTLER, J. (2023). What is synthetic sample- and is it all it's cracked up to be? Kantar. <https://www.kantar.com/inspiration/analytics/what-is-synthetic-sample-and-is-it-all-its-cracked-up-to-be>

Además, se reconoce que el correcto uso de datos sintéticos podría vencer ciertos desafíos a los que las empresas se enfrentan, como las limitaciones presupuestarias, los riesgos de privacidad y escasez de datos.

Finalmente, el 89% de los encuestados reconocieron estar usando herramientas impulsadas por inteligencia artificial en sus tareas diarias y el 83% de las empresas planean aumentar significativamente su inversión en herramientas de inteligencia artificial¹².

Pero, el uso de datos sintéticos no se encuentra libre de riesgos ni consideraciones claves que se deben seguir, lo cual implica que un uso inadecuado podría gatillar diversos riesgos. Entre los principales riesgos identificados están aquellos que vulnerarían la privacidad de la información utilizada para entrenar a la inteligencia artificial, los cuales eventualmente podrían ser reidentificados, o también la reproducción de sesgos existentes en los datos originales, que puedan existir al momento de crearlos, lo cual podría llevar a obtener resultados discriminatorios.

Si bien estos riesgos serán desarrollados más adelante, es importante tener en el radar estos puntos.

En principio, el desarrollar datos sintéticos que sirvan como muestras representativas implica que sean diseñados por profesionales expertos tanto en el uso de herramientas de inteligencia artificial, como en estadística y diseño de datos; de lo contrario la herramienta empleada podría no procesar correctamente los datos de muestra y terminar cayendo en las ya conocidas alucinaciones de los modelos de lenguaje de gran tamaño (LLM por sus siglas en inglés *Large Language Model*).

De igual forma, cuando se determine utilizar modelos de aprendizaje automatizados se debe tomar en cuenta que estos empleen medidas de seguridad suficientemente eficientes para resguardar la confidencialidad de los datos personales ingresados al momento de su entrenamiento; caso contrario, se podrían ver expuestos a brechas de seguridad que derive en las divulgaciones de la información consecuencia de una posible reidentificación, es decir comunicar los datos personales utilizados.

¹² Qualtrics. (2024). AI to drive massive changes to market research in 2025, Qualtrics Report Says. Qualtrics.

Otra consideración al momento de emplear datos sintéticos es que estos sean entrenados con datos personales exactos y representativos, de lo contrario, se corre el riesgo de obtener data inexacta o incluso que conlleven sesgos desde su generación.

Por ello, la calidad del insumo que se utilice, en este caso los datos de entrenamiento deben ser de alta calidad y representativos a fin de garantizar que los modelos de inteligencia artificial empleados logren reproducir datos confiables y útiles, en especial en el caso de testeo de piezas publicitarias, en donde las decisión se basan en patrones de comportamiento de consumidores.

Sobre este punto, consideramos relevante compartir una publicación realizada por Kantar, en la cual se realizó una prueba comparativa entre una muestra de datos sintética versus respuestas humanas reales, para lo cual emplearon un LLM estándar desarrollado por OpenAI como es GPT-4, lo que permitió en este estudio analizar las diferencias en exactitud y sesgos entre datos reales y datos sintéticos.

Los resultados obtenidos en esta prueba concluyeron que GPT-4 tiene un fuerte sesgo positivo en comparación con las obtenidas de los humanos encuestados, en especial en aquellas relacionadas a afirmaciones subjetivas como lo es la emoción que le puede generar un producto; mientras que cuando se trata de afirmaciones objetivas, como lo sería el precio de un producto, el resultado es más preciso.

Así, aún cuando los datos sintéticos pueden reaplicar patrones, existen ciertas limitaciones como los sesgos inherentes a los datos originales (Kalidas & Ostler, 2023)¹³.

Finalmente, un hecho no menor, es que los resultados de preferencia obtenidos con el empleo de datos sintéticos no deberán ser utilizados para comunicar supuestos resultados de percepción de consumidores sobre el uso de los productos.

En efecto, lamentablemente suelen darse casos en los que se observan piezas publicitarias engañosas que comunican porcentajes de resultado

¹³ KALIDAS, A., & OSTLER, J. (2023). What is synthetic sample- and is it all it's cracked up to be? Kantar. <https://www.kantar.com/inspiration/analytics/what-is-synthetic-sample-and-is-it-all-its-cracked-up-to-be>

sobre un supuesto beneficio, cuando en realidad se tratan de estadísticas de preferencia de los consumidores.

Sin embargo, si se emplean datos sintéticos para obtener estos resultados estadísticos, se estaría cometiendo un acto de engaño, toda vez que, mediante el empleo de data no obtenida en su integridad de un estudio de preferencia de los consumidores, se buscaría inducir a error sobre los beneficios de un producto.

Este tipo de acciones en el Perú podrían ser calificados como un acto de engaño, conforme a lo regulado a nivel peruano en el Decreto Legislativo N.1044, Ley de Represión de la Competencia Desleal.

V. Reflexión final: ¿es necesario regular el uso de datos sintéticos en Perú?

Hasta el momento hemos analizado el uso de los datos sintéticos como herramienta de evaluación en el lanzamiento de campañas publicitarias, así como los beneficios y riesgos que su uso inadecuado podría implicar. De igual forma hemos visto como algunas jurisdicciones han considerado necesario pronunciarse de forma directa, como en el caso de la Autoridad de Singapur, o de forma indirecta, como se muestra en la guía emitida por la Autoridad de datos del Reino Unido.

Frente a ello, resulta pertinente cuestionar si es necesario que en el Perú se regule de forma expresa el uso de datos sintéticos, tomando en cuenta que ya se vienen empleando numerosas herramientas de inteligencia artificial no solo en la elaboración de piezas publicitarias, sino en la mayor parte del desarrollo de productos.

Desde la evaluación desarrollada en este artículo, consideramos que, si bien, no será necesario emitir una norma específica que regule como tal el uso de datos sintéticos, es recomendable que se emita una guía que permita empezar a conocer con mayor profundidad los datos sintéticos, incluyendo definiciones claras sobre el concepto, criterios para su creación, técnicas para reducir el riesgo de brechas de seguridad y recomendaciones sobre gobernanza de procesos.

Esto permitirá que tanto grandes como pequeñas empresas puedan incorporar los datos sintéticos de forma segura en sus procesos, sin dejar de lado aquellos mecanismos de mejora de la privacidad de los datos que se utilicen como fuente de entrenamiento.

En ese sentido, el contar con esta guía fomentaría la innovación y competitividad de la industria mediante el uso de datos sintéticos, logrando optimizar tiempo y reduciendo las posibilidades de que los datos personales de entrenamiento sean revelados como consecuencia de una brecha de seguridad e infrinjan la Ley de Datos Personales.

Consideramos que esta propuesta seguiría la ruta ya trazada por otras jurisdicciones, pero adaptándolo al contexto regulatorio peruano, sin que ello implique frenar el uso de herramientas innovadoras.

VI. Conclusiones

El uso de datos sintéticos en la industria del marketing viene cobrando mayor relevancia, en especial como una herramienta para agilizar la etapa de validación del mensaje publicitario, lo cual permitiría a las empresas evaluar diferentes estrategias sin que implique un uso de datos personales como tal.

Así, los resultados evaluados a lo largo del presente artículo arrojan un panorama alentador para su uso, desplegando múltiples de beneficios como podría ser la mejora en la eficiencia de procesos de análisis y reducción de costos versus la disminución de riesgos de privacidad.

Sin embargo, su uso no está exento de posibles riesgos que podría enfrentar, los cuales podrían ir desde sesgos en los modelos que se entrenen hasta reidentificación de los datos personales usados como entrenamiento; lo cual, a su vez, impactaría en el objetivo de testeado que se pretende obtener.

Por ello, diversas jurisdicciones vienen orientando a los usuarios a través de la emisión de guías o lineamientos de buenas prácticas, como la guía publicada por la PDPC de Singapur o el ICO del Reino Unido, ofrecen una orientación para la generación de datos sintéticos de forma responsable con el objetivo de reducir los riesgos de seguridad que su uso conllevaría.

Sin perjuicio de ello, en tanto los datos sintéticos configura una herramienta que se encuentra en constante evolución y que los avances en el uso de inteligencia artificial son cada vez más rápidos, es evidente que de implementarse una regulación rígida podría limitar la evolución, lo cual no sería la forma más adecuada de enfrentar los riesgos de privacidad u otros riesgos que aun no hayan sido detectados.

En especial en aquellos países como el Perú, donde no se observa un vasto desarrollo ni se han identificado plenamente cuáles serían los riesgos. Por ello, sería más beneficioso optar por tener un enfoque flexible y que sirva para educar al mercado.

De esta forma, podría ser de mayor utilidad promover la implementación de guías explicativas o recomendaciones y buenas prácticas para su uso, incluyendo incluso pautas para su aplicación considerando la privacidad, seguridad, mitigación de sesgos y auditoría de riesgos, con el objetivo de que las empresas puedan adentrarse al mundo de los datos sintéticos de forma responsable.

Consideramos que esta propuesta lograría fomentar la innovación sin perder de vista la obligación de respetar los datos personales.

Inteligencia Artificial en la Publicidad Digital: Desafíos Regulatorios y Protección del Derecho de los consumidores

Jasmin Rojas Canales* y Próspero Martín Cortez**

Resumen.- Este artículo analiza los desafíos regulatorios derivados del uso de inteligencia artificial en la publicidad digital. Aborda los riesgos sobre la privacidad, la competencia desleal y la transparencia de los algoritmos publicitarios, proponiendo un marco normativo que garantice la protección de los derechos fundamentales y la equidad en el mercado.

Palabras Clave.- Inteligencia artificial - Consentimiento - Publicidad.

Abstract.- This article analyzes the regulatory challenges arising from the use of artificial intelligence in digital advertising. It addresses the risks related to privacy, unfair competition, and the transparency of advertising algorithms, proposing a regulatory framework that ensures the protection of fundamental rights and equity in the market.

Keywords.- Artificial intelligence - Consent - Advertising.

* Bachiller en Derecho por la Universidad Peruana de Ciencias Aplicadas con mención en Gestión y Liderazgo. Actualmente, practicante profesional de la Sala Especializada en Eliminación de Barreras Burocráticas del INDECOPI.

** Abogado por la Universidad de Lima. Candidato a Magister en Derecho de Administrativo Económico por la Universidad del Pacífico. Especialista en Derecho publicitario, competencia desleal y protección al consumidor. Actualmente, miembro de la Dirección Legal de Competencia y Relaciones de Consumo de América Móvil Perú S.A.C. (CLARO PERÚ).

I. Introducción

El presente trabajo examina los desafíos que plantea la publicidad digital basada en inteligencia artificial respecto al consentimiento para el tratamiento de datos personales.

En el Perú, la Ley 29733 – Ley de Protección de Datos Personales y su Reglamento establecen que dicho consentimiento debe ser informado, previo y expreso; de igual forma, el Código de Protección y Defensa del Consumidor reconoce el derecho a la información como garantía esencial de los usuarios. Sin embargo, en la práctica, esta aceptación suele producirse de manera apresurada y automática, sin una comprensión real de los términos involucrados. Ello genera un desfase entre el consentimiento formalmente otorgado y la voluntad materialmente informada de los consumidores.

Una visión conservadora sostiene que, si el usuario no lee lo que acepta, las consecuencias derivadas de esa omisión son de su entera responsabilidad. No obstante, una postura garantista –la que se adopta en esta investigación– considera que el ordenamiento jurídico debe ofrecer mecanismos que aseguren un consentimiento auténtico, comprensible y consciente. Este enfoque no implica favorecer al consumidor en detrimento de las empresas, sino alcanzar un equilibrio que otorgue mayor autonomía informativa al usuario y, a la vez, brinde seguridad jurídica a las compañías sobre la legitimidad del tratamiento de los datos que recopilan.

La problemática se intensifica en el ámbito de la publicidad digital personalizada, donde los algoritmos de inteligencia artificial procesan grandes volúmenes de datos para segmentar perfiles y dirigir anuncios a medida. Mientras las empresas sostienen que cuentan con autorización válida, numerosos usuarios cuestionan haberla otorgado, lo que evidencia un vacío entre la apariencia de consentimiento y la efectiva voluntad informada. Esta dinámica plantea un reto regulatorio de gran relevancia: garantizar que la personalización comercial no se convierta en una práctica invasiva o carente de transparencia.

En este escenario, el trabajo propone la implementación de una cláusula dinámica, concebida como un mecanismo contractual que permita a los usuarios gestionar, de manera clara y flexible, qué datos comparten y

con qué fines específicos. De esta forma, se busca superar la aceptación automática de políticas extensas y poco comprensibles, reforzando la autonomía del consumidor y legitimando el uso de la inteligencia artificial en la publicidad digital bajo parámetros de transparencia, equidad y confianza.

II. La Inteligencia Artificial en la Publicidad Digital

La inteligencia artificial ha revolucionado la forma en que se diseña y distribuye la publicidad digital, al permitir un nivel de segmentación y personalización sin precedentes. A través del análisis masivo de datos (*big data*), los algoritmos identifican patrones de consumo, predicen preferencias y elaboran perfiles detallados de los usuarios, transformando la publicidad en un mecanismo cada vez más preciso y dirigido. Este avance tecnológico, sin embargo, plantea un reto jurídico de gran relevancia: garantizar que la innovación no se desarrolle al margen de la transparencia, la equidad y la tutela efectiva de los derechos de los consumidores.

Actualmente, resulta evidente que el internet se ha convertido en el medio más intensivo para la difusión de publicidad, desplazando progresivamente a los canales tradicionales. Es altamente probable que quien lea este artículo reconozca que recibe la mayor parte de los anuncios a través de internet, ya sea durante la navegación en redes sociales o en otros espacios digitales.

En el caso peruano, los datos evidencian este cambio de paradigma. Según la Compañía Peruana de Estudios de Mercados y Opinión Pública (CPI)¹ en 2024 la inversión en publicidad digital representó el 36,2 % del total de gasto publicitario, superando por primera vez a la televisión como principal medio de difusión comercial. Esta tendencia refleja una realidad ya consolidada a nivel internacional, donde desde hace varios años la publicidad digital constituye el canal predominante. La importancia económica del sector explica, a su vez, el creciente interés de las empresas por perfeccionar sus estrategias digitales mediante el uso

¹ Compañía Peruana de Estudios de Mercados y Opinión Pública. (2025). Evolución de la Inversión Publicitaria en el Perú 2020 - 2024. Obtenido en: <https://www.cpi.pe/images/upload/paginaweb/archivo/26/CPI%20-%20Market%20Report%202025%20-%20Inversion%20Publicitaria.pdf>

de inteligencia artificial, orientadas a maximizar la rentabilidad de sus campañas publicitarias:

Medios	2020	2021	2022	2023	2024
Digital	27.1%	33%	33.7%	34.5%	36.2%
TV	42.5%	41%	38.3%	36.8%	33.5%
Radio	10.4%	8.8%	9.1%	9.6%	9.6%
Publicidad exterior	6.8%	6%	7.5%	8.4%	9.5%
Diarios digitales	3.6%	3.7%	4.1%	4.4%	4.7%
Diarios impresos	5.7%	4.2%	4.3%	3.7%	3.2%
Cable	3.4%	3.1%	2.9%	2.6%	2.5%
Cine	-	-	-	-	0.5%
Revistas	0.5%	0.2%	0.2%	0.2%	0.2%

(Cuadro de elaboración propia)

Este fenómeno evidencia cómo la publicidad digital, inicialmente vista como un complemento, se ha consolidado como el principal canal de comunicación comercial. A nivel global, el dominio de este medio es indiscutible y ha impulsado la creación de mecanismos cada vez más sofisticados para difundir anuncios personalizados. Los tradicionales anuncios genéricos que aparecían de manera indiscriminada han sido reemplazados por sistemas capaces de dirigir mensajes únicamente a quienes, con base en el procesamiento de datos, se consideran receptores potencialmente interesados.

La pregunta clave es: ¿cómo logran las empresas conocer tales preferencias? Las vías son múltiples. El internet de las cosas recopila información personal cuando, por ejemplo, un usuario comparte su reporte de actividad física a través de una pulsera inteligente (*smartband*), o cuando permite a aplicaciones de movilidad como Waze acceder a su ubicación en tiempo real. Del mismo modo, cada interacción en redes sociales, navegadores de búsqueda o plataformas de comercio electrónico genera datos valiosos: desde el uso de una palabra clave en Google, hasta la compra de un producto en Amazon o Temu. Toda esta información,

proporcionada de manera constante por los usuarios, se convierte en insumo estratégico para la publicidad digital personalizada.

Como dice Endara (2023), “el impacto de la publicidad programática en la personalización de anuncios es innegable, redefiniendo la manera en que las marcas interactúan con sus audiencias”².

Un ejemplo ilustrativo: un gimnasio podría dirigir anuncios específicos únicamente a personas que realizan actividad física en un horario determinado, en una zona geográfica concreta, e incluso mostrar promociones vinculadas al equipamiento que más utilizan en su entrenamiento. De esta forma, la publicidad deja de ser aleatoria para convertirse en un proceso altamente segmentado y estratégico.

Este proceso de personalización se fundamenta en el *big data*, es decir, en la recopilación y procesamiento de grandes volúmenes de información sobre los consumidores. Si bien existen diversas prácticas empresariales orientadas a este fin, en este trabajo nos centramos en aquellas que utilizan inteligencia artificial para el tratamiento del *big data*.

Un caso comúnmente experimentado por los usuarios es el siguiente: se realiza una búsqueda en Facebook sobre impresoras y, al poco tiempo, aparecen múltiples anuncios relacionados no solo en dicha red social, sino también en otras plataformas digitales. Este fenómeno es resultado de un proceso de automatización que combina *machine learning* e inteligencia artificial. A partir de la información obtenida de nuestras interacciones, los algoritmos realizan predicciones de comportamiento y presentan publicidad ajustada a esos intereses.

Ambas herramientas cumplen funciones complementarias:

- *Machine learning*: se encarga de procesar y clasificar la información derivada del *big data*, generando predicciones sobre el comportamiento de los usuarios.
- Inteligencia artificial: permite transformar esas predicciones en estrategias publicitarias más complejas, adelantándose a las necesidades de los consumidores y diseñando anuncios ajustados a sus perfiles.

² Endara Chimborazo, Juan Carlos. (2023). *Impacto de la publicidad programática en la personalización de anuncios*. Obtenido de: <https://www.editorialsphaera.com/index.php/hor/article/view/15/93>.

En este sentido, la inteligencia artificial aplicada a la publicidad digital no solo debe analizarse como un avance tecnológico, sino también como un desafío regulatorio. Su desarrollo exige mecanismos claros y dinámicos que garanticen que la innovación se despliegue de manera responsable, respetando los derechos de los consumidores y asegurando transparencia en el tratamiento de sus datos. Alcanzar este equilibrio es indispensable para evitar que el progreso tecnológico derive en prácticas invasivas que erosionen la confianza de los usuarios, y para garantizar, al mismo tiempo, que las empresas actúen en un marco jurídico predecible y legítimo.

La práctica de recopilar datos para la elaboración de perfiles constituye precisamente el núcleo del problema que se examinará en el siguiente apartado.

III. Desafíos Regulatorios Actuales

La creciente sofisticación de la inteligencia artificial aplicada a la publicidad digital plantea retos regulatorios sustantivos en torno a la recopilación, el tratamiento y la utilización de datos personales. Como se explicó previamente, los algoritmos que predicen preferencias, intereses y hábitos de consumo han reemplazado a la publicidad tradicional, permitiendo niveles inéditos de segmentación a partir del uso intensivo de Big Data. No obstante, este modelo descansa sobre una base frágil: la escasa comprensión que tienen los consumidores respecto del uso real de su información y de las consecuencias que ello genera en su vida digital.

En efecto, aunque la personalización de contenidos puede representar un beneficio para la experiencia del usuario —al hacer más relevante y eficiente la publicidad recibida—, el proceso que la sustenta suele estar rodeado de opacidad. El consumidor desconoce cómo, para qué y por cuánto tiempo se emplean sus datos, lo que genera una brecha entre su expectativa de privacidad y la realidad de su exposición digital. La asimetría de información es evidente: mientras las plataformas disponen de herramientas sofisticadas para extraer y procesar datos, los usuarios aceptan políticas de privacidad extensas, con lenguaje técnico o interfaces que inducen a una aceptación irreflexiva.

A pesar de que la personalización puede representar un beneficio para la experiencia del usuario —al hacer más relevante y eficiente el contenido que se le muestra—, la lógica detrás de su implementación se encuentra

revestida de opacidad, lo que impide al consumidor ejercer control sobre su entorno digital.

Esto se agrava cuando la recopilación de datos se genera sin que el usuario comprenda cómo, para qué y por cuánto tiempo se utilizarán dichos datos, generando así una disociación entre su expectativa de privacidad y la realidad de su exposición digital.

Al respecto, surge la pregunta ¿Es la publicidad dirigida un riesgo que compromete nuestros derechos como consumidores o una herramienta útil de las empresas que podría mejorar nuestra experiencia digital? Para ello, Karina Olano (2025) menciona que, el Reglamento de Datos Personales (art. III.11) define la elaboración de perfiles como el tratamiento automatizado que predice o analiza aspectos del comportamiento de una persona. Sin embargo, esto solo es válido si se informa claramente al titular que se le aplicará este tratamiento a través de la política de privacidad; se ha otorgado consentimiento expreso; se aplican medidas de seguridad y evaluación de impacto (cuando corresponda). La segmentación de perfiles referido a la publicidad dirigida puede ser una herramienta útil para personalizar la experiencia digital del consumidor para las empresas³.

Sin embargo, ¿los consumidores o usuarios son conscientes de la explotación de sus datos?

A pesar de que una gran mayoría de personas expresa una alta preocupación por el uso indebido de sus datos personales en internet, muy pocas toman acciones concretas para protegerlos, como podría ser invertir un tiempo mínimo en leer las políticas de privacidad que aceptan. Esta contradicción evidencia la llamada “paradoja de la privacidad”, donde existe una brecha entre la preocupación manifestada y el comportamiento real del usuario. Esto ha sido evidenciado por el Servicio Nacional del Consumidor de Chile, donde se concluye que múltiples consumidores admiten nunca leer la política de privacidad de los sitios que visita:

³ Olano, K. (12 de Mayo de 2025). Entrevista Personal. (J. Rojas, Entrevistador)

“Según una encuesta del SERNAC, el 72% de las personas declara estar muy o extremadamente preocupadas de que sus datos personales puedan ser recopilados en internet, sin embargo, sólo el 4,1% de ellas señalan siempre leer las políticas de privacidad”⁴.

Frecuentemente, los usuarios no advierten que acciones cotidianas como una búsqueda en línea o una visita breve a una página web generan huellas digitales que alimentan sistemas algorítmicos. Las *cookies* permiten capturar datos como tiempo de navegación, clics, historial de compras o ubicación, información que posteriormente es procesada para configurar perfiles publicitarios. El problema surge cuando este proceso se lleva a cabo sin un consentimiento plenamente informado, es decir, cuando el usuario accede al uso de cookies de forma automática o irreflexiva, sin comprender las implicancias de su decisión ni el destino de los datos entregados.

En efecto, aceptar *cookies* suele convertirse en una acción meramente instrumental para acceder al contenido, antes que una decisión reflexiva sobre el uso de datos personales.

Esta dinámica evidencia una asimetría de información entre las plataformas digitales y los usuarios, quienes se ven enfrentados a mensajes ambiguos, lenguaje técnico o interfaces diseñadas para inducir a la aceptación rápida, debilitando la posibilidad de ejercer un control real sobre su privacidad. En tal contexto, el consentimiento pierde legitimidad como base para el tratamiento de datos, dado que el usuario no ha comprendido el alcance de su elección ni ha participado activamente en ella.

La situación plantea un desafío cuando estos datos ingresan a sistemas algorítmicos que operan bajo estructuras opacas, comúnmente denominadas “cajas negras”. En ellas, los criterios que determinan qué publicidad mostrar, a quién y por qué, no son comprensibles ni verificables por parte del usuario.

Así, la personalización se transforma en un mecanismo de intervención sobre la experiencia digital que actúa de espaldas al consumidor. El

⁴ Servicio Nacional del Consumidor. (2022). Casi la mitad de los consumidores admite nunca leer la política de privacidad de los sitios que visita. Obtenido en: <https://www.sernac.cl/portal/604/w3-article-64751.html>

proceso completo —desde la recopilación mediante cookies hasta la ejecución algorítmica— se desarrolla sin transparencia ni posibilidad de verificación, lo que impide a las personas conocer, cuestionar o corregir los efectos que la segmentación genera sobre sus decisiones y su percepción del entorno digital. Es por ello que el consentimiento que se recaba desde el inicio de la toma de los datos debe ser un consentimiento dinámico y claro, que empoderen sin dificultar la gestión de los datos del usuario.

Lo expuesto, nos clarifica por qué la protección de la privacidad digital representa una preocupación creciente, por ejemplo, entre los estadounidenses, quienes adoptan diversas prácticas para resguardar sus datos personales en línea; pero incluso aquí un estudio realizado por el Pew Research Center revela contradicciones importantes en su comportamiento: si bien una mayoría afirma haber ajustado configuraciones de privacidad en redes sociales o rechazado cookies, también es común que acepten políticas de privacidad sin leerlas, especialmente los adultos jóvenes y aquellos con mayor nivel educativo:

“Alrededor del 56% de los estadounidenses dicen que siempre, casi siempre o a menudo hacen clic en “aceptar” de inmediato, sin leer lo que dicen las políticas de privacidad. Otro 22% dice que lo hace a veces. Y el 18% dice que rara vez o nunca está de acuerdo sin leer”⁵.

Asimismo, es muy probable que exista una percepción generalizada de que las políticas de datos personales no comunican eficazmente cómo se utilizan los datos, por lo que, muchas personas las considerarán como un mero trámite para acceder a los servicios, sintiendo así que leer o no al final no tiene ningún impacto real.

Frente a este panorama, resulta indispensable repensar la forma en que las empresas vienen recopilando el consentimiento de los usuarios en entornos digitales mediados por inteligencia artificial.

La falta de comprensión real y efectiva sobre el uso de cookies y el procesamiento algorítmico de datos no solo pone en entredicho la

⁵ McClain, C., Faverio, M., Anderson, M., & Park, E. (2023, 18 de octubre). How Americans protect their online data and privacy. Pew Research Center. <https://www.pewresearch.org/internet/2023/10/18/how-americans-protect-their-online-data/>

autonomía del consumidor, sino que también evidencia la necesidad de soluciones concretas que garanticen una participación activa, informada y consciente en el ecosistema digital por parte de tales usuarios. En el siguiente capítulo se examinará una alternativa concreta que apunta en esta dirección y, consideramos, garantiza un efectivo consentimiento que termina empoderando al usuario, dándole dinamismo a su aceptación.

Por ello, resulta indispensable repensar los mecanismos actuales de obtención del consentimiento, incorporando soluciones que reconcilien la innovación tecnológica con la protección de derechos fundamentales. El reto no consiste en prohibir la publicidad personalizada —la cual puede aportar valor al mercado y al consumidor—, sino en dotarla de legitimidad a través de un consentimiento verdaderamente informado y dinámico. Solo así será posible superar la tensión entre la eficiencia empresarial y la autonomía del usuario, restableciendo la confianza en un entorno digital que hoy se percibe como opaco y asimétrico.

IV. Propuesta

Considerando todo este contexto, en el presente apartado se propone la creación de una cláusula dinámica para obtener un consentimiento real, orientado a regular de manera clara, transparente y verificable el tratamiento automatizado de datos personales y el perfilamiento digital de consumidores en entornos digitales.

En ese contexto, se plantea la incorporación de una cláusula dinámica como mecanismo contractual innovador que permita superar las deficiencias del consentimiento tradicional en entornos digitales. A diferencia de la aceptación genérica de cookies o políticas extensas redactadas en lenguaje técnico, la cláusula dinámica propone un consentimiento granular, interactivo y comprensible para el usuario. Su funcionamiento radica en que los consumidores puedan gestionar de manera diferenciada dos variables esenciales: qué datos se comparten y para qué fines específicos. De este modo, el consentimiento dejaría de ser una formalidad vacía para convertirse en un verdadero ejercicio de autonomía informativa, complementando —y no sustituyendo— las exigencias legales vigentes.

Esta cláusula surge como una respuesta frente a un escenario donde el consentimiento, en su forma actual, se ha vaciado de contenido

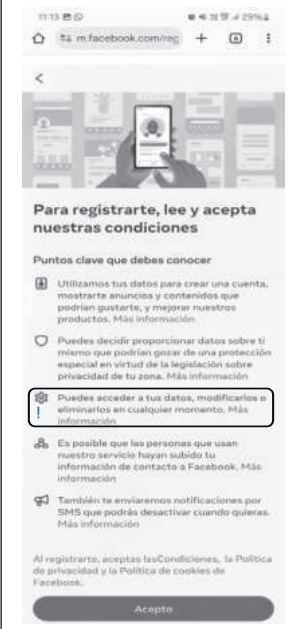
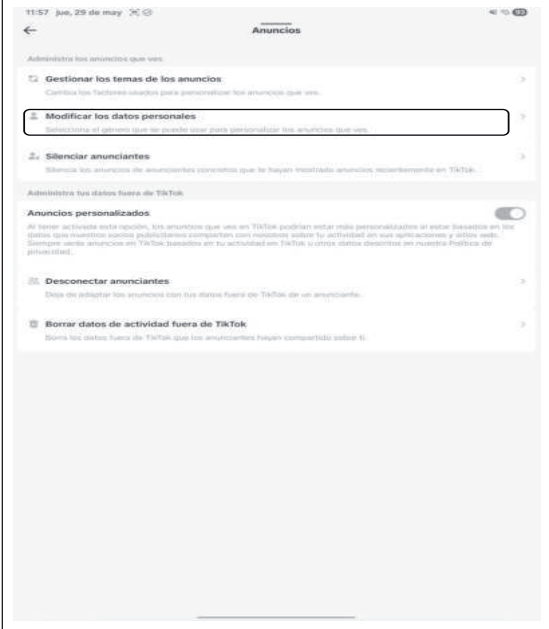
sustancial. El modelo predominante, basado en la aceptación genérica de cookies o políticas de privacidad, se ha vuelto ineficiente para garantizar que los usuarios comprendan qué datos se recopilan y para qué uso.

En la práctica, el consentimiento informado se ha convertido en una formalidad. Los usuarios se enfrentan a formularios extensos, redactados en un lenguaje técnico o ambiguo, y a interfaces que privilegian la aceptación inmediata —mediante botones preseleccionados o ventanas emergentes persistentes— como condición para acceder a servicios digitales. Esta arquitectura persuasiva no sólo desincentiva la lectura crítica, sino que refuerza patrones de aceptación automática. El resultado es un consentimiento que, si bien existe jurídicamente, es inválido desde una perspectiva sustantiva y real, ya que se otorga sin comprensión, sin libertad real y sin alternativas viables de oposición. A esto se suma el hecho de que muchas plataformas digitales están configuradas por defecto para maximizar la recolección de datos, sin brindar información adecuada ni permitir ajustes accesibles para el usuario.

Este problema estructural se agrava en el contexto de la llamada “paradoja de la privacidad”, que revela una brecha entre la preocupación expresada por los usuarios respecto al uso indebido de sus datos personales y las acciones concretas que toman para protegerlos. Aunque la mayoría afirma sentirse incómoda con prácticas intrusivas de recopilación de información, son muy pocos quienes leen políticas de privacidad, ajustan configuraciones o se informan sobre los usos reales de sus datos.

Frente a este panorama, la cláusula dinámica que aquí se propone busca estandarizar y rediseñar el mecanismo mediante el cual se informa, solicita y valida el consentimiento del usuario para el tratamiento de datos con fines de publicidad personalizada. Esta cláusula debería permitir al usuario habilitar o deshabilitar el uso de determinado datos y para un determinado uso. Estas dos variables son las que realmente le interesaría al usuario poder gestionar: Dato y Uso. El resto de información sobre los datos personales bien pudiese encontrarse en un apartado de información complementaria. Esta cláusula debiese ser dinámica y clara.

A continuación, algunas empresas que ya usan cláusulas dinámicas:

Facebook (Meta)	Tik Tok
 11:13 m.facebook.com/reg Para registrarte, lee y acepta nuestras condiciones Puntos clave que debes conocer - Utilizamos tus datos para crear una cuenta, mostrarte anuncios y contenidos que podrían gustarte, y mejorar nuestros productos. Más información - Puedes decidir proporcionar datos sobre ti mismo que podrán gozar de una protección especial en virtud de la legislación sobre privacidad de tu zona. Más información Puedes acceder a tus datos, modificarlos o eliminarlos en cualquier momento. Más información - Es posible que las personas que usan nuestro servicio hayan subido tu información de contacto a Facebook. Más información - También te enviaremos notificaciones por SMS que podrás desactivar cuando quieras. Más información Al registrarte, aceptas las Condiciones, la Política de privacidad y la Política de cookies de Facebook. Acepto	 11:57 Jue, 29 de mayo Anuncios Administra los anuncios que ves Gestionar los temas de los anuncios: Controla los factores usados para personalizar los anuncios que ves. Modificar los datos personales Selecciona el idioma que se puede usar para personalizar los anuncios que ves. Silenciar anunciantes Silencia los anuncios de anunciantes con los que te hayas interesado. Recomendados en TikTok. Administra tus datos fuera de TikTok Anuncios personalizados Al tener activada esta opción, los anuncios que ves en TikTok podrían estar más personalizados al estar basados en los datos que nuestros socios publicitarios comparten con nosotros sobre tu actividad en sus aplicaciones y sitios web. Siempre verás anuncios en TikTok basados en tu actividad en TikTok, u otros datos descritos en nuestra Política de privacidad. Desconectar anunciantes Deja de adaptar los anuncios con tus datos fuera de TikTok de un anunciante. Borrar datos de actividad fuera de TikTok Borra los datos fuera de TikTok que los anunciantes hayan compartido sobre ti.

Como se aprecia, estas empresas poseen una buena práctica para la recopilación de los datos personales pues desde el registro (como es el caso de Facebook) o después del mismo (como es el caso de TikTok) empodera al usuario para modificar de manera personalizada el uso de sus datos y usos según vean conveniente haciendo click en “Más información” o en un determinado “botón”. Repetimos, una cláusula no tipo pero sí dinámica que como mínimo permita gestionar los datos y los usos para el tratamiento y elaboración de perfiles.

La implementación de esta cláusula no solo permitiría reducir la asimetría de información que actualmente existe entre empresas y usuarios, sino que también contribuiría a fortalecer la legitimidad del uso de inteligencia artificial en contextos comerciales, promoviendo un ecosistema digital más ético, inclusivo y respetuoso de los derechos del consumidor.

En este contexto, ya no basta con incorporar una casilla de verificación al final de una política extensa y poco comprensible. Es necesario avanzar hacia mecanismos más dinámicos, interactivos y comprensibles que permitan al usuario participar activamente en el proceso de toma de decisiones sobre su privacidad. El consentimiento debe dejar de ser una formalidad legal vacía para convertirse en una herramienta real de control ciudadano sobre su información personal. En otras palabras, esta cláusula dinámica no solo permitiría cumplir con los requisitos legales formales, sino que se traduciría en una real protección del derecho a la protección de los datos personales bajo una experiencia tangible y efectiva para los individuos en el entorno digital.

V. Conclusiones

El análisis demuestra que, en la práctica, el consentimiento otorgado por los usuarios en entornos digitales es un acto mayormente formal, carente de una verdadera deliberación consciente. La mayoría de titulares de datos personales acepta cláusulas extensas sin leerlas, con el único fin de acceder a la plataforma o continuar con el servicio digital. Este comportamiento pone en evidencia una paradoja: aunque el ordenamiento jurídico peruano ya reconoce derechos fundamentales como el consentimiento informado y los derechos ARCO, su efectividad se diluye en la práctica cotidiana.

Frente a ello, la investigación propone la adopción de cláusulas dinámicas, entendidas como instrumentos que permitan al usuario autorizar o denegar, de manera clara y específica, el tratamiento de un dato o el uso concreto de este, ya sea al crear una cuenta o durante la navegación. La innovación no recae en el contenido —pues los derechos ya están previstos en la ley—, sino en la forma de presentación y gestión continua del consentimiento, que debe ser simple, accesible y comprensible.

Este modelo implica reconceptualizar el consentimiento digital como un proceso deliberativo y dinámico, en contraposición a su carácter declarativo y estático. La propuesta no busca negar la utilidad de la publicidad personalizada ni frenar la innovación tecnológica; por el contrario, plantea un marco que fortalezca la autonomía informativa del consumidor, garantizando que las decisiones sean más conscientes y equilibrando la eficiencia empresarial con la tutela de los derechos fundamentales.

Ahora bien, la viabilidad de este modelo exige que su implementación no dependa únicamente de plazos rígidos impuestos unilateralmente por el regulador. Resulta indispensable un diseño adaptado a la realidad peruana, que considere las capacidades y limitaciones de las empresas. En este sentido, un esquema que combine incentivos regulatorios y gradualidad, en lugar de sanciones inmediatas, permitiría una transición ordenada hacia un consentimiento digital más legítimo y efectivo.

Más allá de la dimensión normativa, la incorporación de cláusulas dinámicas también debe analizarse desde una perspectiva estratégica. En un mercado cada vez más competitivo y sensible al tratamiento de los datos personales, las empresas que adopten prácticas transparentes y respetuosas no solo cumplirán con la ley, sino que también fortalecerán la confianza del consumidor, mejorarán su reputación corporativa y obtendrán una ventaja competitiva sostenible. En este contexto, el consentimiento genuino se convierte en un activo intangible que legitima el uso de la inteligencia artificial en la publicidad digital.

Finalmente, la investigación invita a reflexionar sobre la necesidad de integrar el análisis jurídico con una comprensión más amplia de los efectos sociales y tecnológicos de la inteligencia artificial. La publicidad personalizada, si se desarrolla bajo parámetros de transparencia, deliberación y equidad, puede consolidarse como una herramienta legítima y eficiente. De lo contrario, corre el riesgo de profundizar la desconfianza social en la tecnología y de erosionar los derechos fundamentales de los consumidores. La clave, por tanto, radica en avanzar hacia un modelo en el que innovación y protección de derechos no se perciban como fuerzas en tensión, sino como dimensiones complementarias de un ecosistema digital justo y sostenible.

Brechas digitales e inteligencia artificial: Retos en el acceso a la justicia

Ivan Alexander Polo Olivarez*

Resumen.- La creciente brecha digital, ignorada por el deslumbramiento hacia la inteligencia artificial, obstaculiza la digitalización ordenada de la justicia. Esta investigación analiza cómo la implementación tecnológica sin planificación genera nuevas barreras para los justiciables. Se analiza que la digitalización y la inteligencia artificial deben ser accesibles para fortalecer la equidad y efectividad del acceso a la justicia, en lugar de convertirse en nuevos obstáculos.

Palabras clave.- Brecha digital - acceso a la justicia - digitalización de la justicia - inteligencia artificial - barreras tecnológicas.

Abstract.- The growing digital divide, often ignored amidst artificial intelligence advancements, hinders the orderly digitalization of justice. This paper analyzes how unplanned technological implementation creates new barriers for those lacking digital resources or skills. It argues that accessible digitalization and AI in the justice system are crucial for strengthening equity and effective access, rather than becoming new obstacles.

Keywords.- Digital divide - Access to Justice - Digitalization of Justice - Artificial Intelligence - Technological Barriers.

* Estudiante de la Facultad de Derecho de la Universidad Continental. Asistente Académico en el Estudio Olivas Flores & Abogados. Participante en el Call for Papers de las XXVIII Jornadas Iberoamericanas de Derecho Procesal: “Los desafíos de los sistemas de justicia en Iberoamérica”, organizado por la Pontificia Universidad Católica del Perú y el Instituto Iberoamericano de Derecho Procesal.

I. Introducción

El acceso a la justicia es un derecho fundamental que asegura la tutela efectiva de los derechos de las personas dentro del marco del Estado Constitucional de Derecho. No obstante, en Perú este derecho se ve gravemente afectado por la brecha digital, especialmente en los sectores más vulnerables de la población.

Este estudio, con un enfoque cualitativo, exploratorio y descriptivo, analiza el acceso a la justicia desde una perspectiva integral, teniendo en cuenta el papel del Poder Judicial y otros actores clave en su garantía. Basado en el marco conceptual del Programa de Naciones Unidas para el Desarrollo (PNUD), se abordan las barreras digitales existentes dentro del sistema judicial, así como los desafíos que surgen de la transformación digital en este ámbito.

La hipótesis central que se plantea sostiene que la brecha digital no solo limita el acceso a la justicia, sino que también refleja un problema estructural de descoordinación interinstitucional y deficiencias en la implementación de políticas públicas destinadas a mejorar el acceso pleno al entorno digital. La digitalización, aunque presenta un gran potencial como herramienta para mejorar el acceso a la justicia, podría profundizar las desigualdades existentes si no se asegura previamente un acceso equitativo a la tecnología para toda la población.

El trabajo se estructura en tres secciones: la evolución del derecho de acceso a la justicia, el análisis de la brecha digital y el impacto de la digitalización y la inteligencia artificial en el sistema judicial peruano. A través de este enfoque, se busca ofrecer una reflexión crítica que permita identificar los principales desafíos y proponer posibles mejoras en la garantía de este derecho fundamental.

II. Acceso a la Justicia y sus principales obstáculos

Junto con el dinamismo histórico de la sociedad y con la llegada del Estado Constitucional de Derecho, la mirada al derecho fundamental del acceso a la justicia ha ido teniendo cambios en la forma en la que este se concibe. En un inicio, como menciona el maestro Priori, la dogmática tradicional hacía referencia a este derecho como el “derecho de acción”,

el cual fue objeto de críticas por el contenido que este comprendía¹. Así, posteriormente con la llegada del Estado Constitucional de Derecho, se concibió una mirada más amplia de este derecho, gestando el “derecho de acceso a la justicia” el cual, era solo visto como un derecho integrante al derecho a la Tutela Jurisdiccional Efectiva.

Sin embargo, con el fin de entender la mayor proporción que ha de abarcar el derecho del acceso a la justicia, no solo como un derecho integrante del derecho a la tutela jurisdiccional efectiva, el Programa de Naciones Unidas para el Desarrollo (PNUD) ha planteado dos enfoques sobre el acceso a la justicia: El **enfoque institucionalista**, centrado en la administración de justicia, y el **enfoque integral**, que lo concibe como un derecho amplio que debe garantizarse en todas las esferas del Estado².

De esta forma, La Rosa Calle, con la visión antes planteada sobre el acceso a la justicia ha mantenido una perspectiva con mayor extensión de dicho derecho, mencionando, por ejemplo, que:

Este es el enfoque más apropiado para la realidad de nuestros países, ya que supone el punto de partida más completo para describir los serios problemas que se presentan cuando no se satisfacen las necesidades jurídicas de la población tradicionalmente excluida ni la forma como podrían ser mejor abordadas³.

En este sentido, con ese enfoque más amplio, el PNUD ha definido el derecho al acceso de la justicia como: “La capacidad de todas las personas, sin distinción de género, edad, raza, identidad sexual, ideología política o creencias religiosas, de obtener respuestas efectivas a sus necesidades jurídicas”⁴. Este concepto abarca no solo la existencia de un marco normativo adecuado que garantice los derechos ciudadanos,

¹ PRIORI POSADA, G. (2019). *El proceso y la tutela de los derechos*. Fondo Editorial de la Pontificia Universidad Católica del Perú.

² Programa de las Naciones Unidas para el Desarrollo. (2005). *Manual de políticas públicas para el acceso a la justicia*. Ediciones del Instituto. <https://inecip.org/wp-content/uploads/INECIP-Manual-Pol%C3%9Cticas-Publicas-Acceso-a-la-Justicia-1.pdf>

³ LA ROSA CALLE, J. (2009). *El acceso a la justicia como condición para una reforma judicial en serio*. Derecho PUCP, (62), pp. 115-128.

⁴ Programa de las Naciones Unidas para el Desarrollo. (2005). *Manual de políticas públicas para el acceso a la justicia*. Ediciones del Instituto. Ediciones del Instituto.

sino también la disponibilidad de información sobre estos derechos y el acceso a asesoramiento en asuntos legales cotidianos en todas las jurisdicciones. Además, implica la existencia de mecanismos accesibles y eficientes para la resolución de conflictos, ya sean gestionados por el Estado o por otras entidades⁵.

Así pues, este enfoque permite reconocer al Estado y a otras entidades tanto públicas y privadas como responsables de garantizar el derecho de acceso a la justicia, desplazando la responsabilidad exclusiva del Poder Judicial. En otras palabras, las patologías del acceso a la justicia deben identificarse desde una perspectiva más integral, que contempla tanto el funcionamiento del sistema jurídico como los diversos actores que lo componen para así determinar los factores que inciden sobre su mal desempeño. De esta forma, en la siguiente sección se va a analizar el funcionamiento de la brecha digital en el acceso a la justicia desde este enfoque integral, para posteriormente identificar de que forma la inteligencia artificial puede tener consecuencias en este aspecto.

III. Brecha digital en el acceso a la justicia

La brecha digital se ha concebido como una manifestación de la desigualdad social que trasciende las barreras económicas o la falta de infraestructura, pues también está vinculada a la ausencia de competencias y formación en el ámbito digital. Esta limitación restringe la capacidad de aprovechar plenamente las tecnologías de la información y la comunicación (TIC), obstaculizando una integración efectiva en la sociedad digital en constante evolución⁶.

Sobre este punto, Cabral ha precisado que:

La brecha digital no sólo se manifiesta en la disponibilidad de tecnología, sino también en la alfabetización digital. Muchas personas, incluidos los abogados, jueces y ciudadanos en general, pueden carecer de las competencias necesarias para interactuar con las plataformas judiciales digitales. Esto crea una barrera adicional para el ejercicio del derecho de defensa y la contradicción procesal⁷.

⁵ *Idem*.

⁶ Organización Internacional del Trabajo. (s.f.). Brecha digital. <https://www.oitinterfor.org/digitalizacion/brecha-digital>

⁷ CABRAL, A. (2025). *Proceso judicial electrónico y digitalización de la justicia en Iberoamérica: Diagnostico y propuestas*. Los desafíos de la Justicia en Iberoamérica.

Así, para el estudio de que como funcionan estas brechas digitales, Van Dijk⁸ ha mencionado que, el acceso a los medios digitales, como computadoras e internet, mantienen un proceso que requiere de cinco fases para estar completamente integrado⁹.

En primer lugar, se encuentra la motivación y actitud, el cual constituye el punto de partida y se refiere a la disposición que tiene el individuo para utilizar las tecnologías digitales¹⁰. En el aspecto del acceso a la justicia, esto implicaría la conciencia de la existencia de recursos y servicios digitales en línea y la voluntad del usuario para emplearlos, es decir, la desconfianza en los sistemas digitales y las tecnologías de la información actúa como supresor del acceso a los medios digitales y por lo tanto limita al sistema de justicia digital.

La segunda fase se centra específicamente en el acceso físico a las computadoras e internet, es decir, en la disponibilidad de dispositivos que permitan el uso del entorno digital¹¹. En Perú, este acceso físico se presenta como uno de los aspectos más complicados de abordar, debido a su crecimiento desequilibrado según la región natural. Tal es así, que, a nivel de 2023, se evidencia que solo el 18.7% de la población de la región Selva tenía al menos una computadora, el 26.1% en la región Sierra y el

Relatos Generales de las XXVIII Jornadas Iberoamericanas de Derecho Procesal. Pontificia Universidad Católica del Perú, pp. 375- 405.

⁸ JAN VAN DIJK es profesor de Ciencias de la Comunicación en la Universidad de Twente, Países Bajos, donde ocupa la cátedra en Sociología de la Sociedad de la Información. Investiga los aspectos sociales de las tecnologías de la información y la comunicación desde 1985. Es presidente del Centro de Estudios en Gobierno Electrónico y su investigación se centra en cuestiones sociales, culturales y políticas, y ha publicado varios libros, entre los que destacan *The Network Society* (1999, 2006, 2012), *Digital Democracy* (2000), *The Deepening Divide: Inequality in the Information Society* (2005), y *Digital Skills, Unlocking the Information Society* (2014), coescrito con Alexander van Deursen.

⁹ VAN DIJK, J. (2020). *Closing the digital divide: The role of digital technologies on social development, well-being of all and the approach of the COVID-19 pandemic* [Presentación de la conferencia]. Virtual Expert Group UN Meeting on “Socially just transition towards sustainable development: The role of digital technologies on social development and well-being of all”, Nueva York, EE. UU.

¹⁰ *Idem.*

¹¹ *Idem.*

42.2% en la región Costa¹², lo que revela la profunda disparidad que existe en este aspecto. Este punto, evidentemente tiene repercusión directa sobre el acceso a la justicia digital ya que se trata de una desigualdad donde la presentación de escritos por una mesa de partes virtual, la consulta de información jurídica en línea y la participación en audiencias virtuales no pueda ser desarrollada de forma efectiva por los justiciables.

La tercera fase está relacionada con el desarrollo de las habilidades digitales, lo que implica la adquisición de competencias necesarias para utilizar eficazmente las tecnologías digitales¹³. Sobre este aspecto, Cabral ha señalado que la preocupación en algunos sistemas jurídicos es mayor sobre la capacitación y formación de los abogados, que no poseen las habilidades requeridas para el uso de herramientas digitales, siendo posibles causas la falta de formación, la falta de medios materiales, alguna discapacidad o la edad avanzada¹⁴.

Al respecto, y teniendo en cuenta el análisis desarrollado sobre el enfoque integral del acceso a la justicia, sostenemos que el estudio de las habilidades digitales debe entenderse desde un enfoque en el que el conocimiento sobre el uso adecuado de las TIC sea equivalente a las necesidades que presentan todos los actores que integran el sistema judicial, incluyendo jueces, abogados, fiscales y todas aquellas personas que requieran conocimientos básicos, intermedios o avanzados para poder avanzar a la siguiente fase del acceso a la justicia en relación con el uso de estas tecnologías.

¹² Instituto Nacional de Estadística e Informática. (2023). *Hogares que tienen al menos una computadora, por años, según ámbitos geográficos*. <https://m.inei.gov.pe/estadisticas/indice-tematico/households-with-access-to-information-and-communic/>

¹³ VAN DIJK, J. (2020). *Closing the digital divide: The role of digital technologies on social development, well-being of all and the approach of the COVID-19 pandemic* [Presentación de la conferencia]. Virtual Expert Group UN Meeting on “Socially just transition towards sustainable development: The role of digital technologies on social development and well-being of all”, Nueva York, EE. UU.

¹⁴ CABRAL, A. (2025). *Proceso judicial electrónico y digitalización de la justicia en Iberoamérica: Diagnostico y propuestas*. Los desafíos de la Justicia en Iberoamérica. Relatos Generales de las XXVIII Jornadas Iberoamericanas de Derecho Procesal. Pontificia Universidad Católica del Perú, pp. 375- 405.

De este modo, la cuarta fase esta referida al uso de las aplicaciones tecnológicas, la cual esta referida a poder utilizar, habiendo adquirido las competencias necesarias, aquellas aplicaciones y plataformas digitales de las cuales buscamos obtener beneficios. Siendo esta última -los beneficios-, la postrera fase, la cual se centra en la búsqueda de resultados tangibles derivados del uso de las tecnologías digitales¹⁵. En el contexto del acceso a la justicia, sostenemos que esta última fase resulta ser aquella sobre la cual se espera que los ámbitos que generan una justicia tardía mejoren, tal es el ejemplo de expectativa de la reducción de la carga procesal con una justicia digital.

En ese sentido, se entiende que cada uno de estos procesos constituye un paso a lograr para el completo acceso y uso de los medios digitales, evidenciando que el proceso de acceso digital no puede ser incoherente con su objetivo final de búsqueda de beneficios, por lo cual resulta imperioso que el estudio de la brecha digital aborde cada una de estas fases y su aplicación escalonada para no generar más desorden y desigualdad. De lo contrario, aquellos que ya enfrentan dificultades en el acceso a la justicia digital podrían verse aún más perjudicados por un crecimiento tecnológico desordenado.

En consecuencia, resulta imperioso mencionar que la brecha digital ocasionada por el crecimiento desordenado de la tecnología en el acceso a la justicia afecta dos dimensiones. Por un lado, aumenta la vulnerabilidad de los sectores más desfavorecidos, quienes no logran beneficiarse de los avances tecnológicos en el ámbito judicial. Por otro, amplía la brecha de poder entre grandes y pequeños despachos jurídicos, dado que los primeros cuentan con acceso a herramientas tecnológicas avanzadas que optimizan la prestación de sus servicios¹⁶.

Por lo tanto, resulta fundamental que el análisis de la brecha digital en el acceso a la justicia se dirija a las políticas de transformación digital en el ámbito judicial en todas las fases antes expuestas y no solo se centren en la modernización tecnológica, sino que también garanticen un acceso equitativo y el desarrollo de competencias digitales. De lo contrario, la

¹⁵ *Idem.*

¹⁶ CASTILLEJO MANZANARES, R. (2022). *Digitalización y/o Inteligencia Artificial*. En S. Calaza López & M. Llorente Sánchez-Arjona (Dirs.), *Inteligencia Artificial Legal y Administración de Justicia*. Editorial Aranzadi, S.A.U., pp. 55-90.

brecha digital seguirá reproduciendo desigualdades estructurales, en lugar de reducirlas.

IV. Inteligencia Artificial y Brecha

En el ámbito del Derecho y su ejercicio, la inteligencia artificial (IA) ha sido objeto de estudio y de miradas optimistas sobre su uso. Así pues, en la academia internacional se ha venido estudiando las formas en las que la IA puede impactar al proceso judicial como herramienta para jueces y demás operadores jurídicos. Tal es el caso de las contribuciones que puede realizar al ámbito probatorio en tres aspectos fundamentales: la revisión de los criterios para la valoración de la prueba, la formulación de hipótesis y, potencialmente, la determinación con menor carga subjetiva de los denominados “estándares probatorios”, como resultado directo del proceso de construcción de hipótesis¹⁷.

Ahora bien, en Perú, la IA ha sido adoptada con la Ley N.º 31814 del 2023, Ley que promueve el uso de la inteligencia artificial en favor del desarrollo económico y social del país. Este dispositivo normativo ha decretado que la IA y las tecnologías emergentes sean de interés nacional en las diferentes actividades económicas y sociales a las que puede contribuir, definiendo a los sistemas basados en IA como: “Sistema electrónico-mecánico que puede, para una serie de objetivos definidos por humanos, hacer predicciones, recomendaciones o tomar decisiones, influenciando ambientes reales o virtuales. Está diseñado para funcionar con diferentes niveles de autonomía”.

De este modo con esta mirada centrada en las tecnologías emergentes, en el país de estudio, el Poder Judicial ha implementado un “asistente virtual” con sistema de Inteligencia Artificial llamado “Curia” el cual se realizó por medio de la Quinta Sala de Derecho Constitucional de la Corte Suprema y está diseñado para optimizar el servicio judicial en términos de celeridad procesal, transparencia y predictibilidad¹⁸.

¹⁷ NIEVA FENOLL, J. (2022). *Inteligencia artificial y proceso judicial: Perspectivas ante un alto tecnológico en el camino*. En S. Calaza López & M. Llorente Sánchez-Arjona (Eds.), *Inteligencia Artificial Legal y Administración de Justicia*. Thomson Reuters (Legal) Limited, pp. 417-437.

¹⁸ Redacción El Peruano. (2024). *Curia: IA optimiza resoluciones*. El Peruano. <https://elperuano.pe/noticia/266227-curia-ia-optimiza-resoluciones>.

Esta iniciativa, se ha celebrado por gran parte del sistema judicial, ya que, en apariencia, esta nueva herramienta serviría de forma tal, que la fundamentación jurídica vendría con mucha reducción en el tiempo de análisis, contribuyendo así a la estudiada función auxiliar de la IA, la cual se manifiesta como el apoyo que se brinda al juez y demás operadores jurídicos humanos, para el mejor ejercicio de sus funciones jurisdiccionales específicas¹⁹.

No obstante, si bien, luce de forma muy deseable un sistema judicial implementado con un sistema de predictibilidad que pueda reducir la carga procesal garantizando mayor seguridad jurídica. Resulta inexorable que se verifique la situación actual de la justicia en Perú y sus intentos por digitalizarla.

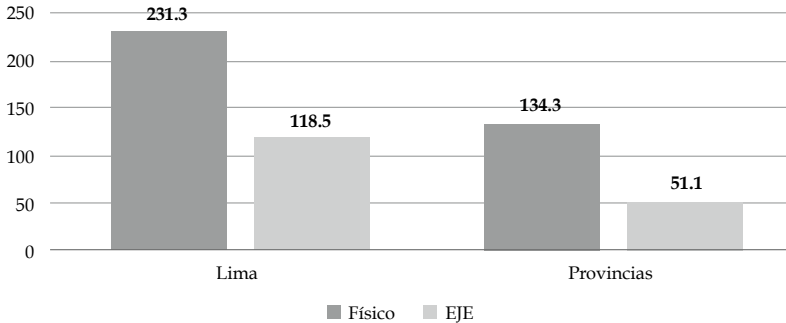
En los últimos años, el sistema de justicia en Perú ha experimentado un proceso de transformación digital con la incorporación progresiva de diversas plataformas electrónicas. Sin embargo, la crisis sanitaria derivada de la pandemia aceleró drásticamente la implementación de estas herramientas, exigiendo su despliegue a nivel nacional en un tiempo mucho menor al originalmente previsto. Este contexto, se impulsó la adopción de soluciones digitales como la Consulta de Expedientes Judiciales (CEJ), el Expediente Judicial Electrónico (EJE), el Servicio de Notificaciones Electrónicas (SINOE) y la Mesa de Partes Electrónica (MPE), entre otras. Aplicaciones que, a la actualidad, se han convertido en instrumentos esenciales para el ejercicio de la abogacía ya que su implementación obligatoria a raíz del COVID-19 permitió que se aprecie la utilidad de estas aplicaciones en la cotidianidad. Así pues, aunque aún persisten desafíos logísticos y operativos para su consolidación total, la emergencia sanitaria demostró la necesidad de fortalecer estos mecanismos digitales para garantizar un acceso efectivo a la justicia²⁰.

De esta forma, según la Organización para la Cooperación y el Desarrollo Económico (OECD), El EJE redujo significativamente la duración de los casos en comparación con las presentaciones físicas en papel, especialmente en las zonas rurales. Por ejemplo, en casos de primera

¹⁹ BARBERIS, M (2024). *Separación de poderes y justicia digital*. Palestra Editores, pp. 125.

²⁰ PRADO BRINGAS, R., & ZEGARRA VALENCIA, F. (2020). *Debido proceso en tiempos de pandemia. En Derecho de los Desastres: COVID-19*. Pontificia Universidad Católica del Perú, pp. 731-732.

instancia, las Cortes Superiores del Departamento de Lima tardaban 223 días en cerrar un caso mediante el expediente físico. Con el EJE, se necesitan 222,4 días (-un 0,3 % de reducción de tiempo). Las Cortes Superiores de las provincias tardaban 131,1 días en cerrar un caso con el expediente físico; mediante el EJE, necesitan 75,6 días (-un 42 % de reducción de tiempo)²¹.



Fuente: Organización para la Cooperación y el Desarrollo Económico (OECD). (2024, p. 151). *Estudio de la justicia de la OCDE en el Perú: Hacia instituciones de justicia eficaces y transparentes para un crecimiento inclusivo*. OECD Publishing.

En ese sentido, la digitalización de la justicia podría reducir la carga procesal y el tiempo de resolución de los casos sometidos al Poder Judicial. No obstante, respecto de las otras aplicaciones tecnológicas antes mencionadas, resulta inquietante señalar que, entre los años 2022 y 2024, el Poder Judicial ha registrado un total de 317 (trescientos diecisiete) reportes sobre el funcionamiento de la plataforma “Consulta de Expedientes Judiciales” (CEJ). Entre dichos reportes se señalan fallas en la búsqueda de expedientes, errores en la descarga de resoluciones, problemas en la visualización de actuaciones procesales, entre otros. Misma suerte corre, aunque de forma mucho más amplia, en el caso de la Mesa de Partes Electrónica (MPE), donde se han contabilizado 13,707 (trece mil setecientos siete) reportes, los cuales se refieren a incidencias en el ingreso de demandas, la generación de cargos de presentación, dificultades en la búsqueda del expediente al que debe adjuntarse el

²¹ Organización para la Cooperación y el Desarrollo Económico (OECD). (2024). *Estudio de la justicia de la OCDE en el Perú: Hacia instituciones de justicia eficaces y transparentes para un crecimiento inclusivo*. OECD Publishing, pp. 151. <https://doi.org/10.1787/e32675d5-es>.

escrito judicial, entre otros.²² En este contexto, resulta ostensible afirmar que las tecnologías de la información que resultan ser cotidianas en el ejercicio del derecho aún mantienen dificultades para su disfrute completo, se podría sostener entonces, que el beneficio esperado de estas plataformas no se puede materializar debido a que nos encontramos atascados en la fase del uso de las aplicaciones a causa de quien ofrece el servicio.

Cabe señalar que los datos antes mencionados representan únicamente una parte de las incidencias ocurridas en dicho período, dejando un margen para la denominada cifra negra de incidentes no reportados, así como un posible error en el registro de los reportes consignados. Problema que también resultan ser objeto de análisis, ya que se trata de una cuestión que ha permanecido constante a lo largo del tiempo, tal es así que la OECD ha indicado que:

A pesar de los recientes avances, la recopilación y el almacenamiento de datos judiciales en el Perú siguen siendo limitada. Aunque la mayoría de las instituciones de justicia tienen sus propias bases de datos de justicia (...) enfrentan múltiples desafíos de recopilación e interoperabilidad. Por ejemplo, las partes interesadas peruanas informaron de que, debido a la falta de estándares unificados para recopilar datos (existe un marco para la recopilación de datos en todas las instituciones de justicia), algunas instituciones de justicia no recopilan esta información o lo hacen de manera limitada, lo que genera datos inexactos o incompletos²³.

De esta forma, y, en nuestra opinión, esta ineficacia de la digitalización de la justicia en Perú se debe a que la implementación de las TIC se está realizando de forma desordenada a las fases de la integración de los medios digitales los cuales han sido expuestos de forma extensiva.

Sobre este punto, la OECD ha evidenciado que, a pesar de los avances en la digitalización del sistema de justicia en Perú, aún no se ha logrado arti-

²² Esta información ha sido obtenida mediante solicitud de acceso a la información pública, la cual fue recibida por el autor de este artículo a través de correo electrónico el 06 de enero de 2025 mediante la Carta N° 000007-2025-SACTD-GG-PJ. Para acceder a estos datos, se puede contactar al responsable a través del correo electrónico: 75545862@continental.edu.pe.

²³ Organización para la Cooperación y el Desarrollo Económico (OECD). (2024). *Estudio de la justicia de la OCDE en el Perú: Hacia instituciones de justicia eficaces y transparentes para un crecimiento inclusivo*. OECD Publishing, pp. 176. <https://doi.org/10.1787/e32675d5-es>.

cular una visión integral respaldada por una estrategia digital unificada y bien coordinada. Hasta el momento, los esfuerzos digitales han estado mayormente enfocados en modernizar los servicios institucionales de justicia, manteniendo un enfoque tradicional en lugar de priorizar las necesidades de la ciudadanía -justicia centrada en la persona-²⁴.

En esa línea de ideas, en Perú, la digitalización de la justicia, y especialmente la búsqueda de su automatización mediante inteligencia artificial, representa un salto de fases del acceso a los medios digitales. Ello, debido a que, los ciudadanos peruanos aún enfrentan un acceso físico limitado a las TIC proporcionadas por el Poder Judicial, debido a errores que dificultan su uso y la brecha digital existente. Sin embargo, lejos de priorizar la garantía de un acceso pleno y la satisfacción de las necesidades básicas de estas plataformas, el Poder Judicial ha decidido centrar sus esfuerzos en una herramienta judicial basada en IA generativa, saltándose directamente a la fase de utilización sin haber asegurado primero el acceso físico, el uso, ni el desarrollo de habilidades digitales suficientes para mejorar la prestación de los servicios. Esta decisión evidencia que un avance apresurado en la digitalización de la justicia, sin considerar previamente las bases fundamentales de acceso y capacitación, puede llevar a un crecimiento desmesurado que deja importantes vacíos sin atender, de modo que, la rapidez con la que se busca implementar la tecnología puede crear huecos significativos en el sistema, dejando problemas sin resolver en el camino.

Por esta razón, proponemos que, la utilización de la IA pueda estar referida a mejorar la recopilación de datos y la gestión de estos, así, con esta tecnología emergente los datos sobre el desempeño que despliegan los jueces y las TIC cotidianas en el ejercicio de la abogacía podrían ayudar a sincerar el real estado en el que nos encontramos respecto de la digitalización de la justicia y con ello poder sectorizar de mejor forma los esfuerzos para mejorar el acceso real a la justicia. Máxime, si la directriz sobre la promoción del desarrollo científico y tecnológico del país, según el artículo 14 de la Constitución Política del Perú de 1993, impone una obligación gradual al Estado para que mediante su forma de gobierno promueva el desarrollo tecnológico del país en todas las áreas, incluyendo el servicio de justicia²⁵.

²⁴ *Idem*.

²⁵ CHEN STANZIOLA, M. & CAVANI, R. (2025). *Inteligencia artificial, sistema de justicia y proceso judicial en Iberoamérica*. Los desafíos de la Justicia en Iberoamérica. Relatos

Cabe resaltar finalmente que, la automatización de sentencias y la búsqueda rápida de jurisprudencia no garantizan que los jueces utilicen dichas herramientas para satisfacer el derecho del justiciable. Actualmente, los jueces ya cuentan con acceso a Internet para “conocer el derecho” y la jurisprudencia actualizada, pero aún persisten prácticas de legalismo y formalismo que buscan dar respuestas aparentes a intereses particulares. Esta búsqueda de automatización, que ahora se manifiesta como un proceso circular, evidencia una vez más que la digitalización de la justicia, al formar parte de una reforma judicial dentro de un sistema ineficiente, solo provoca una insuficiencia automatizada²⁶.

V. Conclusiones

El acceso a la justicia es un derecho fundamental que, en Perú, se ve seriamente limitado por la brecha digital. Sobre todo, la digitalización de la justicia ha sido implementada sin una estrategia clara, lo que ha generado dificultades en el acceso a la justicia. La falta de acceso a recursos tecnológicos y la escasa capacitación han profundizado la desigualdad en el ejercicio de este derecho.

El uso de la inteligencia artificial en el ámbito judicial, si bien presenta oportunidades, también supone riesgos si no se garantiza previamente un acceso equitativo a la tecnología. La modernización del sistema de justicia no debe centrarse solo en la digitalización y automatización de tareas jurisdiccionales, sino también en fortalecer la recopilación de datos que puedan sincerar el estado real del sistema judicial, además garantizar que los avances tecnológicos sean accesibles para toda la población.

En conclusión, el acceso a la justicia en Perú sigue condicionado por problemas estructurales que requieren un enfoque integral. Las reformas judiciales deben priorizar la equidad y la accesibilidad, asegurando que la digitalización y la inteligencia artificial sean herramientas que reduzcan brechas en lugar de ampliarlas.

Generales de las XXVIII Jornadas Iberoamericanas de Derecho Procesal. Pontificia Universidad Católica del Perú, pp. 309- 372.

²⁶ PÁSARA, L. (2014). *Una reforma imposible. La justicia latinoamericana en el banquillo*. Fondo Editorial de la Pontificia Universidad Católica del Perú.

Criminalidad en tiempos de ChatGPT: Análisis del uso de la Inteligencia Artificial como agravante penal en el Perú

Giacomo Sanguineti*

Resumen.- El autor analiza la Ley 32314, la cual incorporó el uso de inteligencia artificial y tecnologías análogas como agravante penal y modalidad específica en ciertos delitos. Este artículo analiza su legitimidad bajo los criterios de subsidiariedad y necesidad de pena, y examina las capacidades institucionales requeridas para una aplicación efectiva, así como los beneficios y riesgos de dicha ley.

Palabras clave.- Inteligencia Artificial – Agravantes Penales – Delitos Informáticos – Deepfakes – Evidencia Digital – Política Criminal – Perú.

Abstract.- The author analyzes Law 32314, which incorporated the use of artificial intelligence and similar technologies as a criminal aggravating factor and specific modality in certain crimes. This article analyzes its legitimacy under the criteria of subsidiarity and necessity of punishment, and examines the institutional capacities required for effective implementation, as well as the benefits and risks of such a law.

Keywords.- Artificial Intelligence – Criminal Aggravating Factors – Cybercrime – Deepfakes – Digital Evidence – Criminal Policy – Peru.

* Estudiante de Derecho en la Universidad del Pacífico. Integrante del equipo técnico del despacho de asesores de la Tercera Vicepresidencia del Congreso de la República del Perú. Asociado de la Revista de Derecho Forseti. Miembro del Comité de Calidad de la Facultad de Derecho de la Universidad del Pacífico. Presidente del Centro de Estudiantes de la Universidad del Pacífico (CEUP). Asistente de docencia del curso de Derecho Penal General de la Universidad del Pacífico.

I. Introducción

A este punto resulta innegable la expansión que ha tenido la inteligencia artificial (IA) en un sinfín de áreas que inciden en el día a día de las personas¹. La impresionante capacidad de esta tecnología para replicar funciones humanas con una velocidad fuera de nuestras posibilidades, que van desde la realización de tareas cotidianas hasta procesos mucho más complejos, han forzado a que el Derecho se encuentre en la obligación de responder con la mayor rapidez y eficacia que le sea posible ante los desafíos éticos y las nuevas modalidades delictivas que ha traído consigo.

En ese contexto, el Perú ha dado un interesante pero significativo paso con la reciente aprobación de la Ley 32314² mediante la cual

¹ Respecto a lo que se entiende por IA, resulta complicado elaborar una definición unánime, ya que esta puede ser entendida de diversas maneras, dependiendo del enfoque que se adopte. No obstante, la Organización para la Cooperación y el Desarrollo Económico ha conceptualizado el término de Sistema de Inteligencia Artificial en: (OECD). *Hola, mundo: La Inteligencia Artificial y su uso en el sector público*. Documentos de trabajo de la OECD sobre Gobernanza Pública, Núm. 36. 2019, pp. 204-206. <https://oecd-opsi.org/wp-content/uploads/2020/11/OPSI-AI-Primer-Spanish.pdf> de la siguiente manera:

Un sistema basado en máquinas que puede, para un conjunto determinado de objetivos definidos por el ser humano, hacer predicciones, recomendaciones o tomar decisiones que influyen en entornos reales o virtuales. Los sistemas de IA están diseñados para funcionar con diversos niveles de autonomía. Además, las IA son “máquinas que realizan funciones cognitivas similares a las de los seres humanos”.

Asimismo, para tener una mayor comprensión sobre cómo la IA incide en los distintos ámbitos de las vidas de las personas, se recomienda consultar Comisión Europea. *Propuesta del Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de Inteligencia Artificial (Ley de Inteligencia Artificial)* y se modifican determinados actos legislativos de la Unión. 2021, p.1. https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0008.02/DOC_1&format=PDF

² En el Perú los avances sobre propuestas normativas vinculadas a la inteligencia artificial son relativamente recientes, razón por la cual se ha empezado a desarrollar relacionada directamente con la Guía sobre la Inteligencia Artificial. Es con base a dichos avances que resulta novedosa la aprobación de la Ley 31813, Ley que promueve el uso de la inteligencia artificial en favor del desarrollo económico y social del país, cuyo artículo 3 establece que la inteligencia artificial debe entenderse como “Tecnología emergente de propósito general que tiene el potencial de mejorar

se introduce la utilización de la IA como circunstancia agravante en diversas conductas punibles, tanto en el Código Penal como en la Ley de Delitos Informáticos (aprobada mediante la Ley 30096)³. Esta decisión aprobada por el Congreso de la República refleja una respuesta directa a la creciente utilización maliciosa de la tecnología como las falsificaciones profundas (las denominadas “*deepfakes*”⁴), la manipulación multimedia y otras modalidades emergentes de delitos potenciados por IA.

A partir de esta respuesta del Estado peruano, se ha podido evidenciar que, si bien el boom del uso de la IA se ha producido tan solo hace algunos años, rápidamente este se ha convertido en un mecanismo instrumentalizado por personas malintencionadas para causar daño a terceros y vulnerar bienes jurídicos que el Código Penal busca a toda costa proteger. En ese sentido, la relevancia de esta regulación radica no solo en un reconocimiento formal del potencial impacto que puede tener la IA sobre la gravedad de determinados delitos, sino que también representa un mensaje simbólico respecto de la intencionalidad del Estado para adaptar el marco jurídico a uno que sea capaz de dar respuesta a los desafíos tecnológicos actuales.

Sin embargo, cualquier tipo de adaptación normativa no va a estar libre de complejidades y puntos críticos. En particular, en este tipo de propuestas siempre se van a presentar cuestionamientos respecto de cuál va a ser el tipo de concepto que se va a adoptar de inteligencia artificial, qué se va a entender por “tecnologías análogas”, los mecanismos probatorios que

el bienestar de las personas, contribuir a una actividad económica global sostenible positiva, aumentar la innovación y la productividad, y ayudar a responder a los desafíos globales clave”.

³ Específicamente, el nombre completo de la referida norma -la cual fue publicada en el Diario Oficial El Peruano con fecha 29 de abril de 2025- es Ley 32314, Ley que modifica el Código Penal, Decreto Legislativo 635, y la Ley 30096, Ley de Delitos Informáticos, para incluir el uso de la inteligencia artificial en la comisión de delitos.

⁴ Como tal, las *deepfakes* son entendidas como un tipo de manipulación digital de contenido, el cual tiene como elemento esencial el utilizar la IA para crear videos, audios o imágenes que simulan de manera extremadamente realista a personas diciendo o haciendo cosas que en realidad jamás ocurrieron. Debe tenerse en cuenta que estas resultan particularmente peligrosas en el contexto actual, ya que pueden ser utilizadas como herramienta para engañar, difamar, extorsionar o cometer fraudes, entre otros delitos, los cuales no son sencillos de detectar.

son necesarios para demostrar su rol en el marco de la comisión de un delito o, en general, si es que es necesaria como tal una regulación de la IA en un escenario en donde esta tecnología recién está empezando a consolidarse en un país como el nuestro.

Ante esta problemática, el presente artículo pretende delinear algunos conceptos esenciales para poder entender los aspectos que abarca la Ley 32314 (en adelante, la ley de IA como agravante), para posteriormente identificar sus implicancias jurídicas y los desafíos que representa, para finalmente brindar algunas ideas sobre posibles soluciones a dichos retos.

II. Criminalidad potenciada por la IA: Análisis de la Ley 32314

i. Antecedente legislativo

La ley bajo análisis tuvo su origen en el Proyecto de Ley 8746/2024-CR, el cual fue presentado a iniciativa del congresista Isaac Mita Alanoca. La fórmula utilizada en el proyecto de ley proponía modificar el Código Penal para (i) incorporar el uso de inteligencia artificial como circunstancia agravante genérica en el artículo 46.2.e y (ii) agravar el delito de estafa mediante la introducción del numeral 7 en el artículo 196-A cuando se empleen voz, imagen, audio o movimiento corporal de terceros con IA⁵.

Respecto a la Exposición de Motivos, esta sustenta la necesidad de intervención penal en la medida que las herramientas digitales se han convertido en un medio para facilitar actividades ilícitas y aprovecharse de las víctimas. Asimismo, la Exposición de Motivos sostiene que ello iría en línea con la expansión del marco normativo en diferentes aspectos vinculados a la IA, tales como las leyes de delitos informáticos⁶ y de ciberseguridad⁷. Además, si bien existe la Ley de Promoción del Uso de

⁵ Si bien la fórmula inicial del Proyecto de Ley hablaba sobre el agravante genérico para diversos delitos, el enfoque sobre tipos específico se encontraba en su totalidad enfocado en la estafa agravada mediante inteligencia artificial, no advirtiéndose la presencia de agravantes en otros tipos penales como el plagio, pornografía infantil, infracción de derechos de autor, etc.

⁶ Ley 30096, Ley de delitos informáticos.

⁷ Ley 31212, Ley de Ciberseguridad. La referida norma también cuenta con su reglamento, aprobado por Decreto Supremo 012-2020-IN.

la IA, aprobado por la Ley 31814, esta es una norma genérica que no contiene ninguna disposición sancionatoria.

En cuanto al contexto que se brinda en torno a la norma, la Exposición de Motivos sitúa la propuesta en un escenario de rápida expansión de la IA: la adopción global de estas tecnologías creció 250% entre 2017 y 2022, y se resalta que el país busca integrar la IA en servicios públicos como educación y seguridad ciudadana. Asimismo, resulta interesante la referencia de que el Perú se ubicaría entre los cinco primeros países de Latinoamérica que más han adoptado este tipo de tecnologías, lo cual justificaría la oportunidad y urgencia para la intervención penal.

En un plano similar, se afirma que la regulación de IA debe tener un impacto transversal en el ordenamiento jurídico, –que implica la creación y actualización de leyes– a fin de asegurar un uso ético y seguro de esta.

Sin dudas, el referido Proyecto de Ley 8746/2024-CR fue la base esencial para poder llevar a cabo la aprobación de la norma bajo referencia, por lo que se procederá a describir brevemente el texto final de la norma, a fin de poder continuar con el análisis respectivo.

ii. Modificaciones introducidas mediante la aprobación de la Ley 32314

La Ley de IA como agravante introduce dos artículos clave y una Disposición Complementaria Final, con un objetivo claro: insertar el uso de la IA y tecnologías similares o análogas como criterio de agravación tanto en el Código Penal, como en la Ley 30096. En términos prácticos, ello habilitaría, cuando corresponda, el incremento de la pena hasta un tercio por encima del máximo legal fijado para cualquiera de los delitos comprendidos en el mismo.

De forma específica, lo esencial de la reforma está en las circunstancias de atenuación y agravación (art. 46): se reformula el literal e) y se incorpora el literal ñ) para convertir el empleo de IA o tecnologías análogas en una agravante genérica, útil cuando el tipo base no prevé expresamente el empleo de dicho componente tecnológico. Así, este cambio actuaría como una “puerta de entrada” transversal a distintos tipos penales para capturar escenarios en los que la tecnología aumenta sustancialmente la lesividad, la escala del daño o la expectativa de impunidad.

Tomando como base la lógica de este criterio general -aunque bajo una lógica distinta- la ley ajusta tipos específicos donde la IA ya viene teniendo impactos prácticos. En delitos contra la libertad sexual, el art. 129-M (pornografía infantil) incluye contenidos generados por IA – como *deepfakes* u otras técnicas de síntesis – para cerrar la brecha entre producción “tradicional” y generación artificial de material. En delitos contra el honor, el art. 132 (difamación) eleva el reproche cuando la falsedad o denigración se difunde mediante contenidos creados por IA, atendiendo al alcance y persistencia que la manipulación automatizada de contenidos puede dar a la lesión reputacional de las personas afectadas. En delitos patrimoniales, el numeral 7 del art. 196-A agrava la estafa cuando el agente manipula voz, imagen o movimiento corporal mediante IA para causar el perjuicio económico, con el foco puesto en clonación de voz y suplantación audiovisual como medios de captación de confianza. Finalmente, en delitos contra los derechos intelectuales, se modifican los artículos 217, 218, 219 y 220 y se incorporan los arts. 220-A, 220-B y 220-C, para sancionar la elusión de medidas tecnológicas y la fabricación o provisión de herramientas o servicios destinados a esa elusión cuando tal conducta sea facilitada por IA, reforzando la tutela frente a automatizaciones que erosionan controles de acceso o integridad de obras.

Por otro lado, la Ley 30096 de Delitos Informáticos es coherente también con este diseño, dado que faculta al juez a aumentar la pena hasta un tercio por encima del máximo legal cuando el agente comete el delito informático empleado herramientas de inteligencia artificial o tecnologías análogas, buscando lograr una armonización entre el tratamiento que se está buscando implementar en el Código Penal y el sistema de delitos informáticos.

Estándares de subsidiariedad y necesidad de la pena: ¿Se encuentra justificada la Ley 32314?

Ahora bien, resulta menester tener en consideración que el solo hecho de que el Perú se presente como un escenario propenso al uso masivo de la inteligencia artificial no justifica, por sí mismo, la necesidad de que el derecho penal deba intervenir sancionando conductas. Al final, en más de una oportunidad se han incluido tipos al Código Penal cuya elaboración no ha pasado por la mejor técnica legislativa, lo que al final termina resultando ineficiente y dejando con una protección nula a los bienes jurídicos que se pretendía cuidar en primer lugar.

La intervención penal del Estado en el marco del crecimiento de la IA en el país debe ser resultado de una reflexión consciente sobre sus costos, beneficios y riesgos. En ese sentido, una modificación del Código Penal debe examinar cuidadosamente la expansión del ius puniendi del Estado. Para ello, es importante evaluar la pertinencia de la presente ley desde los criterios de subsidiariedad y necesidad de la pena⁸.

Al respecto, la subsidiariedad exige recordar que el Derecho penal es ultima ratio, esto es, su intervención debe constreñirse únicamente a los escenarios en los que otros instrumentos -normas extrapenales, políticas públicas, técnicas jurídicas o normas y agravantes ya existentes- resultan insuficientes para contener un incremento real de lesividad o de impunidad. La necesidad de la pena impone, además, que cualquier agravación demuestre idoneidad, ausencia de alternativas menos gravosas y se demuestre que se cumple un criterio de proporcionalidad en sentido estricto.

A fin de aterrizar dichos criterios en esta materia, el examen debe responder, al menos, a tres preguntas encadenadas: (i) si la IA cumple un rol de contribución sustancial en la comisión, la escala u ocultamiento del delito; (ii) si su empleo eleva ex ante el riesgo de lesión del bien jurídico o la expectativa de impunidad más allá de lo ya previsto por la ley vigente; y (iii) si introduce una dificultad probatoria añadida (detección, atribución o trazabilidad) que justifique un mayor reproche. Cuando estas condiciones se cumplen de forma copulativa, la agravación

⁸ Respecto a este concepto, Villavicencio es bastante categórico cuando señala que la doctrina coincide en que la subsidiariedad es una nota distintiva de la respuesta penal. Esto significa que el Derecho penal solo debe activarse cuando los demás instrumentos del ordenamiento y los controles sociales no penales resultan insuficientes; precisamente por la severidad de sus sanciones, los ataques menos graves a los bienes jurídicos deberían de canalizarse, en principio, por vías extrapenales.

La subsidiariedad se complementa con el principio de fragmentariedad, y ambas se ordenan bajo el principio de intervención mínima. Según Villavicencio, esta directriz de política criminal tiene un triple alcance: el Derecho penal debe (i) seleccionar únicamente los ataques de especial gravedad contra el bien jurídico; (ii) tipificar solo una parte de las conductas que en otras ramas ya se consideran antijurídicas; y (iii) excluir del castigo las acciones meramente inmorales.

Para mayor referencia, ver VILLAVICENCIO, F. (2006). Derecho Penal. Parte general. Lima: Grijley.

de conductas ya no es simbólico, sino un ajuste funcional a un *modus operandi* que intensifica el desvalor de la conducta.

Aplicado al artículo 46 como cláusula general, el test se supera siempre que el término “tecnología análoga o similar” no opere como un “cajón de sastre”, sino como una “llave” que permita incluir medios que efectivamente potencian la comisión o dificultan su persecución. La idoneidad es clara si el uso de IA hace posible un ataque a escala o un ocultamiento que el agente no habría logrado con medios ordinarios.

En ese sentido, la necesidad se verifica cuando no existen agravantes previas que puedan abarcar ese plus de riesgo o de impunidad, mientras que la proporcionalidad exige un umbral de aplicación explícito en la motivación judicial, lo cual también resulta necesario por criterios del derecho al debido proceso⁹.

Respecto del conjunto de modificaciones específicas (libertad sexual, honor, patrimonio y derechos intelectuales), el mismo patrón analítico permite una valoración diferenciada sin entrar aún al detalle caso por caso.

En estos bloques, la idoneidad se fortalece porque el legislador identifica fenómenos concretos -tales como síntesis audiovisual artificial, clonación de voz, elusión automatizada de controles- cuyos efectos típicos son la ampliación del daño y la dificultad de realizar trazabilidad sobre la autoría. De ahí que la necesidad se justifica en la medida en que el tipo base o sus agravantes tradicionales no reflejan adecuadamente ese plus de peligrosidad ni la expectativa de impunidad que trae la automatización; y la proporcionalidad se satisface si la agravación se reserva a supuestos donde la IA no es un mero accesorio, sino un factor determinante para la consumación del delito.

Resulta evidente que pueden caber objeciones sobre un eventual solapamiento con agravantes ya previstos; aun así, al tratarse de técnicas

⁹ Un posible cuestionamiento sobre este apartado sería la vaguedad de término en sí. Una situación similar ocurre a las críticas que -salvando las distancias entre el derecho penal y administrativo- tuvo desde sus inicios la cláusula general en la Ley de Represión de la Competencia Desleal. Sin embargo, acotada por el umbral descrito y apoyada en indicios técnicos verificables, lo cual requiere de inversión y desarrollo de capacidades técnicas, la cláusula cumple la función de cierre que persigue.

de generación o manipulación sintética de difícil detección, el ajuste normativo se sostiene siempre que se exija al juez la demostración el nexo causal tecnológico en la motivación.

En cuanto a la regla de aumento en la Ley 30096, su justificación deriva de lo anterior: los ciberdelitos cometen, por definición, su ataque en un entorno donde la IA puede multiplicar velocidad, alcance y opacidad.

De todas maneras, resulta importante advertir que este debería haberse derivado de forma explícita en la misma Exposición de Motivos y no tener que presumirla, por lo que fue una oportunidad perdida. Sin perjuicio de ello, como se ha demostrado en el presente apartado, existe efectivamente una metodología que permite justificar la razón de ser de la Ley de IA como agravante en función de los criterios de subsidiariedad y necesidad de la pena.

En todo caso, la superación de este test no un tema meramente dogmático, sino también operativo: exige capacidades institucionales suficientes en las autoridades pertinentes como la Fiscalía y la Policía Nacional del Perú para constatar el nexo tecnológico y su rol en la comisión del delito. Como mínimos, deberá garantizarse la integridad y preservación de evidencia digital (por ejemplo, con procesos adecuados de *hashing* y cadena de custodia), pericia especializada en análisis audiovisual y de voz, así como protocolos para la recepción de las pruebas. Sin estos estándares, la aplicación de la agravante corre el riesgo de generar inseguridad jurídica.

El criterio central es claro: agravar únicamente cuando la IA aporte una contribución sustancial, un aumento del riesgo y/o daño y añada una dificultad probatoria sustantiva, lo que deberá reflejarse adecuadamente en la motivación de las sentencias en las que deban ser analizados la comisión de estos tipos penales.

iv. Análisis de las implicancias jurídicas y desafíos

Si hay algo que no se puede negar a partir de la incorporación de la Ley de IA como agravante es que es representa un antes y un después en el abordaje regulatorio que va a tener la inteligencia artificial en el Perú. Por un lado, existen posturas más proteccionistas que ven con sospecha a la violenta evolución de la inteligencia artificial, tanto por sus impactos en el entorno laboral relacionado al potencial reemplazo de puestos de trabajo en diversas áreas cuyas labores podrían ser automatizadas (o, en

todo caso, volverlas mucho más productivas con el uso de la IA), como el mal uso que se le ha dado a esta herramienta en múltiples ámbitos, tales como los vinculados al plagio académico o la violación de derechos de propiedad intelectual, entre otros.

Por otro lado, una posición diferente se ve representada por el sector privado y los negocios emergentes –y hasta, en varias oportunidades, el sector público– quienes ven a la inteligencia artificial como un fenómeno revolucionario que vino para quedarse y al que debemos adaptarnos; y mientras antes nos adaptemos, mejor. Esta tendencia más receptiva y liberal hacia la IA ve con buenos ojos el enorme potencial que tiene para mejorar el desarrollo de la colectividad, sobre todo teniendo en cuenta el crecimiento exponencial de la economía digital en los últimos años. De hecho, por la misma redacción de la Ley 31813 y su Proyecto de Reglamento, pareciera ser este el enfoque por el que el legislador ha optado.

Ahora bien, aunque ambas posiciones naturalmente suelen verse enfrentadas, no quiere decir que no puedan –e incluso deban– complementarse en determinados contextos. Es decir, las posiciones previamente descritas no son en ninguna circunstancia excluyentes, por lo que considero que debemos tener una posición en general de apertura hacia la IA, pero a la vez debemos ser capaces de reconocer sus riesgos y de actuar respecto de ellos de forma preventiva, a fin de que las virtudes de la IA puedan convivir con los objetivos de desarrollo del Estado peruano.

Teniendo ello bajo consideración, el hecho de que se haya incluido a la IA como un agravante en el Código Penal y en la Ley de Delitos Informáticos representa una modernización sin precedentes en nuestra legislación penal. A nivel simbólico, la tipificación de la IA en este escenario genera una narrativa por parte del legislador de que no serán tolerables las conductas de todo aquel que procure instrumentalizar esta herramienta para facilitar la comisión de un delito o para ampliar su alcance, razón por la cual la respuesta punitiva del Estado será mayor, buscando reforzar la función preventiva de la norma penal.

De esta manera, podemos apreciar la primera virtud de norma, que es el efecto disuasivo que busca alcanzar. Si lo analizamos desde la perspectiva del transgresor de la norma penal, el empleo de la IA, que en otras circunstancias lo habría ayudado a poder generar *deepfakes*

para extorsionar a otras personas o plagiar una obra, deja de ser un mecanismo rentable.

Ello principalmente se debería a dos motivos: (i) La sanción penal es mayor, por lo que el análisis costo-beneficio del delincuente para ejecutar la conducta sancionable debe necesariamente incluir este factor en la evaluación; y (ii) es posible que aumente la probabilidad de detección si es que el Estado garantiza el empleo de recursos públicos a las instituciones competentes para hacer viable la identificación de estos delitos. En otras palabras, se pretende alterar la balanza de incentivos del infractor, con el objetivo que la IA ya no sea percibida únicamente como un factor que garantiza el anonimato o que puede implicar alguna sanción administrativa (o, en el mejor de los casos, un ostracismo mediático), sino como un factor que hace que la comisión del delito pierda atractivo.

Un segundo tema que merece atención es el hecho de que la reforma combina una agravante genérica, que es la contenida en el artículo 46 del Código Penal, con ajustes específicos en tipos penales concretos relativos a conductas que en la práctica son los que más han sufrido por el incremento en el uso de la IA.

Esta decisión, a menos a mi entender, no es caprichosa o deliberada, sino que es parte de una estrategia de técnica en diseño legislativo que opta por evitar constantes modificaciones normativas cada vez que una nueva herramienta tecnológica que pueda ser catalogada como “análoga” a la IA incida en algún delito. De esta forma, mientras que por un lado se tiene a ciertos delitos que ya contienen el agravante de la IA incorporado en el texto del tipo, en el resto de los casos solo basta verificar que la conducta se encuentre “potenciada por IA” para agravarla.

De todas formas, respecto al artículo 46 en concreto, la aplicabilidad de esta cláusula recae también en la capacidad del Poder Judicial para exigir una motivación reforzada cuando se invoque el uso de IA como agravante. En línea con lo desarrollado previamente, corresponde al juzgador explicitar por qué la tecnología tuvo una contribución sustancial en la comisión, escala u ocultamiento del delito y por qué ese plus no está ya captado por agravantes ordinarias. Tal conclusión debe apoyarse en pericias técnicamente fiables, con metodología identificable, control de errores y adecuada trazabilidad y cadena de custodia.

Un tercer acierto de la norma radica en que es plenamente consciente de los riesgos que la inteligencia artificial implica para determinadas conductas sociales. De un lado tenemos el reconocimiento explícito de fenómenos contemporáneos como lo son los *deepfakes*, por lo que su evaluación en el marco de una investigación penal tendrá cierto nivel de certeza.

De otro lado, las conductas cuyas modificaciones no se ven afectadas por el artículo 46 han sido objeto de constantes y acalorados debates en la actualidad. Por ejemplo, escándalos relativos a la posesión o distribución de pornografía infantil¹⁰, así como las interminables discusiones del rol de la IA en la elaboración de documentos de autoría propia que pueden terminar en plagio¹¹, son situaciones que se dan en el día a día y frente a los cuales la población buscaba una respuesta.

¹⁰ Durante los últimos años, constantemente ha habido escándalos de estudiantes universitarios que han sido capturados por posesión y presunta difusión de pornografía infantil, tal como el caso de un estudiante arequipeño en 2023. LINARES, K. (2023). Universitario de 22 años fue detenido por posesión de pornografía infantil. Diario el Pueblo. <https://diarioelpueblo.com.pe/2023/07/20/universitario-de-22-anos-fue-detenido-por-posesion-de-pornografia-infantil/>.

Aún más sorpresivo, recién el pasado 21 de mayo un estudiante fue detenido en Trujillo por la posesión de videos sexuales en donde aparecerían menores de 13 años, lo cual ha generado gran debate en redes sociales. RAMOS, P. (2025). PJ dicta prisión preventiva para joven universitario tras hallársele 100 mil archivos de pornografía infantil en Trujillo. RPP. <https://rpp.pe/peru/la-libertad/trujillo-dictan-prision-preventiva-para-joven-universitario-tras-hallarsele-100-mil-archivos-de-pornografia-infantil-noticia-1636064>.

Si bien en ninguno de estos casos parte de la discusión se ha encontrado en la utilización de la IA como herramienta que facilite el delito, la norma busca anticiparse ante estos escenarios, a fin proteger los bienes tutelados de libertad e indemnidad sexual de los menores en contextos tan delicados como este.

¹¹ El año pasado, el congresista del Bloque Magisterial, Paul Gutiérrez, fue acusado de copiar y pegar contenido generado por IA en, al menos, la elaboración de dos propuestas legislativas presentadas como si fueran de su autoría. PINEDO, J. (2024). Acusan a congresista Paul Gutiérrez de copiar y pegar respuestas de la inteligencia artificial en sus proyectos de ley. RPP. <https://rpp.pe/politica/congreso/acusan-a-congresista-paul-gutierrez-de-copiar-y-pegar-respuestas-de-la-inteligencia-artificial-en-sus-proyectos-de-ley-noticia-1556672>.

Probablemente el caso más paradigmático, atendiendo al contexto de los últimos meses, es el de la extorsión¹², las amenazas y las estafas¹³, ante las cuales nuestro país lamentablemente se ha visto sumido en una ola de violencia que no parece que vaya a cesar de forma significativa en el corto plazo. En ese sentido, la atención de estas situaciones era necesaria vista la realidad peruana que nos rodea. De esta forma, se espera que esta normativa pueda alcanzar a los referidos actos delictivos en las circunstancias en las que se use IA, a fin de disminuir su reincidencia.

Aunque ello va a depender mucho de la voluntad de los funcionarios públicos, un efecto positivo de este impulso podría estar vinculado con la presión que esta ley ejerce sobre las instituciones públicas encargadas de la persecución penal. Bajo esa línea de argumentación, el convertir a la IA como agravante de un delito “obliga” a la Policía Nacional del Perú, al Ministerio Público y al poder Judicial a reforzar sus conocimientos y capacidades técnicas.

Así, se requiere de peritos especializados, capacitación constante y protocolos de cadena de custodia para el material digital que sean más robustos. A ello se suma la necesidad de contar con una infraestructura tecnológica suficiente (laboratorios forenses, softwares de preservación

¹² Nuestro país durante los últimos meses se ha visto inmerso en una gigantesca ola de violencia. RAMÍREZ, S. Paro nacional para el 14 de mayo: ¿Qué gremios paralizarán y qué servicios no estarán disponibles? El Comercio. <https://elcomercio.pe/lima/paro-nacional-para-el-14-de-mayo-que-gremios-paralizaran-y-que-servicios-no-estaran-disponibles-noticia/>. Redacción EC. (2025). Transportistas de Lima convocan a paro el 10 de abril por creciente ola de extorsiones y violencia. El Comercio. <https://elcomercio.pe/lima/transportistas-de-lima-convocan-a-paro-el-10-de-abril-por-creciente-ola-de-extorsiones-y-violencia-inseguridad-ciudadana-estado-de-emergencia-ultimas-noticia/>.

Si bien el uso de la IA no se da en todos los contextos, la preocupación por esta herramienta sumado al miedo por las extorsiones tradicionales provoca que el miedo colectivo aumente.

Sin perjuicio de ello, el plagio mediante IA es un tema que se ha venido discutiendo en la academia y en la prensa desde hace algún tiempo.

¹³ El fraude digital ha ido cogiendo bastante fuerza en el país, situación que podría empeorar debido a la mayor especialización de los ciberdelinquentes que usan herramientas de inteligencia artificial. MELO, Y. (2025). Fraude digital en Perú: el 90% de limeños teme ser víctima mientras las estafas se vuelven más sofisticadas. Infobae. <https://www.infobae.com/peru/2025/03/24/fraude-digital-en-peru-el-90-de-limenos-teme-ser-victima-mientras-las-estafas-se-vuelven-mas-sofisticadas/>

de evidencia, servidores seguros, etc) y de criterios uniformes de actuación que eviten diferencias arbitrarias entre fiscalías o distritos judiciales. Cuando no se invierte en este tipo de capacidades, la prueba digital termina cuestionada en cualquier instancia del proceso judicial, con el riesgo de absoluciones por fallas técnicas más que por falta de culpabilidad.

Evidentemente, ello implica una importante inversión de los recursos públicos para que dichas competencias puedan ser efectivamente ejercidas, por lo que, volviendo a la idea previa, ello será bastante contingente al compromiso que exista por parte de las instituciones.

Ahora bien, a modo de primera crítica, resulta relevante señalar que la expresión “tecnologías análogas o similares” representan cierto nivel de riesgo para el principio de legalidad y taxatividad. Sin perjuicio de que sus alcances se hayan esbozado en las secciones precedentes de este artículo, no puede negarse que una expresión tan amplia puede colisionar con la predictibilidad en la aplicación de la norma y, ergo, en la seguridad jurídica que debe primar en el derecho penal.

Así, el no contar con una definición clara para estas herramientas, aumenta el riesgo de discrecionalidad con la que los jueces pueden aplicar la norma, vulnerando potencialmente no solo el derecho de defensa, sino aumentando también el riesgo de pronunciamientos contradictorios. Además, teniendo en consideración que la Única Disposición Complementaria Final prevé la emisión de normativa adicional necesaria en el plazo de sesenta días calendarios desde la entrada en vigor de la norma, quedan dudas razonables sobre cómo se van a abordar este otro tipo de tecnologías (sobre todo, teniendo en cuenta que nuestro desarrollo sobre investigación en IA aún es muy incipiente y solemos extraer las definiciones que ya han sido acogidas en otras legislaciones), por lo que uno se podría preguntar, ¿estamos ante una remisión normativa? ¿Se trata de una ley penal en blanco? ¿Respecto de qué otro tipo de tecnologías me podrían sancionar? Dada esta situación, resulta imperante tener una respuesta adecuada.

Otra discusión importante radica en tema probatorio. Primero, los operadores de justicia deben tener cuidado con la interpretación de la norma y ser bastante precisos al momento de determinar que el uso de la inteligencia artificial cumplió un papel trascendental en la comisión de la conducta infractora. El mero uso de una tecnología no necesariamente

aumenta de forma significativa la lesividad de un hecho, pero el riesgo se encuentra en concluir inmediatamente que corresponde la aplicación del agravante. En ese sentido, resulta necesario definir los lineamientos y estándares que serán aplicables para estos casos.

Sobre este mismo punto, debe tenerse en cuenta que la intervención de algoritmos, redes neuronales y *deepfakes* usualmente requieren de pericias avanzadas, acceso a herramientas de análisis forenses especializadas o conservación de evidencias efímeras¹⁴. En la medida que no se cuentan con dichos recursos, o estos son muy limitados, es menester realizar una distribución eficiente del dinero público para invertir en herramientas avanzadas que permiten un verdadero incremento en la probabilidad de detección de estos delitos.

Finalmente, se debe cuidado con el efecto inhibitorio que pueda generar la Ley de IA como agravante sobre la innovación. Si bien resulta positivo que se genere un mensaje de modo que el sector privado tenga cuidado en el desarrollo de software potenciado con IA, ello puede implicar una serie de costos. En principio resulta positivo que la reforma induzca a proveedores y desarrolladores a reforzar autenticación, trazabilidad y políticas de uso responsable de la inteligencia artificial, así como a ser mucho más cuidadosos con la cadena de custodia de información.

No obstante, una regulación excesivamente laxa también genera costos y puede desalentar decisiones empresariales relevantes. Si el marco no es lo suficientemente claro, aumentan los costos de cumplimiento privado preventivos (seguros, auditorías, contratos más restrictivos) y los riesgos ex post (litigios o sanciones reputacionales) por la dificultad de demostrar la diligencia. En ese entorno, empresas prudentes podrían retrasar lanzamientos, limitar funcionalidades sensibles o imponer

14 Piénsese, por ejemplo, en la necesidad de (i) software de análisis de patrones de comprensión o incongruencias de fotogramas para comparar videos sospechosos con bases de datos de rostros o voz originales en el caso de los *deepfakes*; (ii) herramientas de espectrograma o programas de análisis forense de audio clonado; (iii) inspección de redes neuronales en dispositivos incautados para rastrear si es que fueron entrenadas para generar contenido ilícito; (iv) órdenes de preservación rápida con el fin de congelar logs, metadatos y snapshots de las máquinas donde se generaron los archivos; y (v) herramientas de análisis de tráfico de red para tener trazabilidad sobre los flujos de datos que permita rastrear la distribución de *deepfakes*, entre otros.

barreras de acceso a usuarios de mayor riesgo, lo que igualmente impacta en la velocidad de innovación.

En cambio, un marco sólido y predecible —como el que se viene consolidando en materia de ciberdelincuencia— puede operar como señal de certidumbre, dado que alinea expectativas, facilita la debida diligencia con clientes y proveedores y reduce la probabilidad de controversias por zonas grises. El punto no es “más” o “menos” regulación, sino mejor aplicación de la misma: criterios claros de cuándo la IA aporta una contribución sustancial que justifica la agravación, estándares probatorios mínimos y una motivación reforzada que evite sancionar el mero uso tecnológico neutro.

En cualquier caso, se debe tener cuidado con la aplicación de la ley, ya que nuestro ordenamiento aún se encuentra construyendo sus primeros cimientos en regulación de inteligencia artificial, por lo que, si bien la iniciativa se saluda y tiene una serie de puntos a destacar, la cautela siempre será la estrategia más adecuada.

III. Conclusiones

Definitivamente la aprobación de la Ley 32314 marca un punto de inflexión en la política criminal ante la expansión de la inteligencia artificial. La norma moderniza el Código Penal y la Ley 30096 al reconocer que la IA amplifica la velocidad, el alcance y la magnitud de una serie de conductas ilícitas. Debido a ello, la ley presenta un mensaje disuasorio claro; no obstante, la reforma evidencia tensiones inevitables entre la necesidad de proteger bienes jurídicos y el deber de salvaguardar los principios de legalidad, proporcionalidad y seguridad jurídica.

Como se ha explicado a lo largo de la presente investigación, este nuevo régimen presenta algunos riesgos que deben examinarse. Entre ellos, el uso de conceptos como “tecnologías análogas o similares” puede generar cierto grado de incertidumbre normativa; la carga probatoria para demostrar que una conducta ilícita ha sido facilitada o conseguida mediante IA exige de una infraestructura forense difícil de aplicar en nuestro país hoy mismo; y la amenaza de sanciones sin criterios claros podría desalentar algunos proyectos de innovación si es que no existe una armonización con los intereses legítimos del sector privado.

En ese sentido, más allá de los beneficios de la norma que han sido resaltados en el presente trabajo, a fin de mitigar los riesgos se recomienda,

de forma general: (i) Emitir criterios técnicos que delimiten de forma más precisa las circunstancias en las que se configura el agravante o, en todo caso, que la normativa futura que se va a emitir sea lo suficientemente clara en este apartado; (ii) Procurar dotar a los jueces, fiscales y peritos de los recursos necesarios y la capacitación adecuada en temas de inteligencia artificial y cómo combatir su uso para fines ilícitos; y (iii) No descuidar el *soft law*, ya que acompañar este proceso con guías de buenas prácticas o *sandboxes* regulatorios pueden permitir a las empresas desarrollar programas de IA responsable y ética sin el riesgo de que sean penalizados por ello.

En síntesis, la promulgación de esta ley constituye un gesto relevante del legislador frente a los complejos desafíos que plantea el entorno digital contemporáneo. Sin embargo, en el ámbito penal, la aprobación de una norma no puede leerse simplemente como una respuesta coyuntural; debe entenderse como el ejercicio, siempre delicado, del ius puniendi del Estado. Y ese poder, por su misma naturaleza, exige sobriedad, contención y una responsabilidad institucional a la altura de su alcance.

Una política criminal efectiva no se define por la severidad de sus penas ni por la celeridad de su tramitación legislativa, sino por su capacidad de resistir al tiempo, a la presión política y a los vaivenes de la opinión pública. El verdadero equilibrio se alcanza cuando se logra proteger eficazmente a la sociedad sin erosionar los pilares del Estado de Derecho, la seguridad jurídica ni el dinamismo propio de la innovación tecnológica.

Se dice —con razón— que el derecho y la justicia suelen llegar tarde. Y aunque ello sea cierto, más grave aún es que se anticipen sin reflexión, pues pueden terminar lesionando los derechos que buscaban tutelar. En ese sentido, legislar con rigor técnico, con deliberación informada y con conciencia de las consecuencias jurídicas y sociales de cada decisión no es una opción: es una exigencia inherente al mandato constitucional del legislador.

Los sesgos naturales en la programación algorítmica: desafíos y dificultades para la aplicación de sistemas automatizados en el derecho

Gonzalo Renzo Villavicencio Rojas*
Juan Pavel Valdez-Rondinel**

Resumen.- Este artículo examina la inteligencia artificial jurídica y su choque con los sesgos del lenguaje legal. Analiza la automatización y el uso de datos, mostrando cómo pueden institucionalizar discriminaciones estructurales. Se advierte así el riesgo de que la IA se convierta en un instrumento tecnocrático que legitime injusticias bajo apariencia de neutralidad.

Palabras clave.- Inteligencia artificial - sesgo legal - sesgos cognitivos - lenguaje jurídico - sesgo algorítmico - interpretación legal - automatización discriminatoria - justicia tecnocrática - automatización jurídica - jurisprudencia e IA.

Abstract. - This article examines legal artificial intelligence and its clash with biases in legal language. It analyzes automation and data use, showing how they can institutionalize structural discrimination. It warns of the risk that AI becomes a technocratic tool legitimizing injustices under the guise of neutrality.

Keywords.- Artificial intelligence - legal bias - cognitive biases - legal language - algorithmic bias - legal interpretation - discriminatory automation - technocratic justice - legal automation - jurisprudence and AI.

* Estudiante del 7.º semestre de Derecho en la Universidad Peruana de Ciencias Aplicadas.

** Estudiante del 12.º semestre de Derecho en la Universidad Nacional de San Cristóbal de Huamanga. Miembro en Círculo académico Franco-Latinoamericano Lucet Universidad de la Sorbona y del Círculo de Derecho Informático CEDIM Universidad Nacional Mayor de San Marcos. Premio nacional de Mejor Orador del Torneo AYNI Bullard Falla & Ezcurra 2024, articulista en LP así como por la universidad Simon Fraser University.

I. Introducción

i. Contextualización del uso de IA en el derecho penal y otros ámbitos jurídicos

En los últimos años, los sistemas de inteligencia artificial (IA) han comenzado a desempeñar un papel cada vez más protagónico en diversas esferas de la vida social, y el ámbito jurídico no ha sido la excepción. La incorporación de algoritmos en los procesos legales ha propiciado una transformación significativa, especialmente en el derecho penal. **Desde modelos predictivos** – como *DEBATER* de IBM – hasta herramientas que evalúan el riesgo procesal de un imputado, la IA se perfila como un actor muy relevante en la toma de decisiones judiciales.

Sistemas como **COMPAS** en Estados Unidos, o aplicaciones más recientes centradas en la clasificación automática de demandas y precedentes, permiten vislumbrar un panorama donde las máquinas ya no solo asisten, sino que influyen directamente en el razonamiento judicial. Sin embargo, esta automatización jurídica convive con interrogantes fundamentales sobre la neutralidad de los algoritmos y la posibilidad de que decisiones aparentemente objetivas estén atravesadas por estructuras sociales, económicas y culturales profundamente arraigadas. Como señalan Boczkowski y Mitchelstein, los algoritmos –*lejos de ser entes autónomos o neutros*– están íntimamente ligados a quienes los diseñan¹, pues “los algoritmos y la agencia humana no son opuestos, sino que están interrelacionados en el sentido de que los humanos son tan parte del software como el código informático mecánico que se destaca en cualquier definición de algoritmos” (p. 48)². En este sentido, la IA no nace del vacío, sino que es el producto de la historia, la cultura y las formas particulares de lenguaje de quienes la crean.

Como advierte Eubanks, “a menudo tratamos la nueva tecnología como algo ajeno a la historia y al contexto, como el monolito de *2001: Odisea en el espacio*, que aparece de la nada, pero aterriza en un terreno vacío

¹ BOCZKOWSKI, P. Y MITCHELSTEIN, E. (2022). *El entorno digital: Breve manual para entender cómo vivimos, aprendemos, trabajamos y pasamos el tiempo libre hoy* (Ciudad Autónoma de Buenos Aires: Siglo XXI Editora Iberoamericana), pp. 48.

² BUCHER, T. (2018). *If...Then: Algorithmic Power and Politics* (New York: Oxford University Press)

y cambia todo; pero en realidad la tecnología surge de la cultura y vuelve a influir en ella”³. Así, los algoritmos que gobiernan muchas de las decisiones contemporáneas no solo reflejan reglas matemáticas, sino que reproducen las estructuras simbólicas, lingüísticas y políticas que habitan quienes los programan.

ii. Presentación de la tesis

En línea con estas perspectivas, el presente artículo sostiene que los sesgos no son simples errores accidentales o anomalías corregibles mediante ajustes técnicos, sino que constituyen consecuencias estructurales e inevitables derivadas del uso del lenguaje humano en los procesos de programación, decisión y argumentación algorítmica. Dichos sesgos emergen como herencias cognitivas, culturales y lingüísticas que acompañan inevitablemente a todo modelo automatizado entrenado con datos generados por seres humanos.

Desde una perspectiva filosófica, se advertía sobre los límites del lenguaje como medio para representar la realidad: la indeterminación semántica — esto es, la falta de correspondencia fija entre palabras y hechos — impide que el lenguaje sea una herramienta perfectamente transparente, eficaz y neutra⁴. Así, el lenguaje es inherentemente sesgado no solo porque puede ser usado con intencionalidad, sino porque es estructuralmente insuficiente para captar de forma exhaustiva la complejidad del mundo. En el campo algorítmico, esto implica que cualquier codificación basada en lenguaje humano — e incluso los algoritmos lo son — estará afectada, en su base misma, por ambigüedades, omisiones y marcos interpretativos específicos que se construyen bajo la intencionalidad del ser humano que se encuentra detrás del algoritmo.

Además de estos sesgos estructurales o semánticos, existen también sesgos intencionales o funcionales, vinculados a intereses sociales, económicos y políticos. Este sesgo se manifestó, por ejemplo, durante la campaña presidencial de Estados Unidos en 2016, donde la circulación de desinformación estuvo altamente concentrada en pequeños nichos

³ EUBANKS, V. (2018). *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor* (New York: St. Martin’s Press)

⁴ LEITGEB, H. (2023). Ramsification and semantic indeterminacy. *The Review of Symbolic Logic*, Cambridge Press, pp. 900-950.

digitales⁵. Aunque solo el 6% de la información era falsa, el 80% de las noticias falsas fueron vistas por apenas el 1% de los usuarios de Twitter, demostrando que el problema no era tanto la cantidad de desinformación, sino su focalización y circulación estratégica. Esta dinámica evidencia que la información puede ser programada, dirigida y manipulada para responder a fines específicos, revelando que los algoritmos no solo reflejan sesgos pasivos, sino que pueden reproducir estructuras de poder y exclusión activamente.

En efecto, como señala Virginia Eubanks, la tecnología suele presentarse como algo novedoso, disruptivo y ajeno al contexto; sin embargo, “la tecnología surge de la cultura y vuelve a influir en ella”⁶. Es decir, la inteligencia artificial no es neutral: es una materialización algorítmica de las visiones, intereses y estructuras de quienes la crean y aplican. Por ello, programar un algoritmo es también inscribir en él una cierta visión del mundo, sus normas y sus exclusiones.

Estas prácticas tecnológicas no operan en el vacío. Como advierten Earl y Kimport⁷, los medios digitales se han vuelto inseparables de las formas de interacción social y activismo, permitiendo que las narrativas, las decisiones y los comportamientos circulen por canales tanto personales como automatizados. Esta mezcla de acción individual, red social y tecnología de datos genera nuevos escenarios donde la intención política, el diseño técnico y el lenguaje humano convergen para producir decisiones con efectos materiales sobre la vida de las personas.

Finalmente, Hidalgo, investigador de la Universidad de Toulouse, entre otros autores, sostienen que “la información es el producto final de las cosas que se producen con el conocimiento”⁸, ya sea un texto, un video o un bien material. Esta visión refuerza la idea de que todo

⁵ LAZER, D. et al. (2018). The Science of Fake News: Addressing Fake News Requires a Multidisciplinary Effort. *Science*, vol. 359, no. 6380.

⁶ EUBANKS, V. (2018). Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor. *St. Martin's Press*.

⁷ EARL, J. y KIMPORT, K. (2013). Digitally Enabled Social Change: Activism in the Internet Age. *MIT Press*.

⁸ RONEN, S.; GONÇALVES, B.; HU, K.; VESPIGNANI, A.; PINKER, S.; HIDALGO, C. (2014). “Links That Speak: The Global Language Network and Its Association with Global Fame,” *Proceedings of the National Academy of Sciences*, vol. 111, No. 52.

dato es una construcción social, no un reflejo objetivo de la realidad. La programación, en consecuencia, es un acto cargado de subjetividad, cultura y lenguaje, por lo que sus resultados —como los algoritmos usados en procesos judiciales— deben ser evaluados no solo desde su eficiencia, sino desde su capacidad para reproducir o cuestionar estructuras de desigualdad existentes —y, sobre todo, la tan buscada y a veces esquiva imparcialidad—.

En síntesis, este artículo propone explicar y replantear la forma en que se conciben los sesgos en sistemas de inteligencia artificial, especialmente en el ámbito judicial. En lugar de asumir que son fallas corregibles, se plantea que son parte constitutiva del modo en que los humanos —y, por tanto, las máquinas que programan— perciben, interpretan y actúan en el mundo. Este desplazamiento de perspectiva es indispensable para problematizar crítica y maduramente el uso de la IA en decisiones judiciales sensibles, como la determinación de la culpabilidad, la proporcionalidad de la pena o la valoración del riesgo procesal. Si bien la promesa de objetividad algorítmica ha ganado terreno en contextos de sobrecarga institucional o incertidumbre normativa, es urgente reconocer que la programación no elimina los prejuicios humanos; en cambio, los traduce a otro lenguaje, los codifica, y en no pocos casos, los amplifica.

iii. Recorrido del artículo

Para sustentar esta tesis, el artículo está compuesto por tres partes interrelacionadas: en primer lugar, se analizan los **sesgos cognitivos** y su anclaje en la psicología humana como mecanismos mentales de simplificación que, si bien útiles, pueden generar distorsiones sistemáticas en la toma de decisiones.

En segundo lugar, se examina el papel del lenguaje como vehículo principal del sesgo estructural, tanto en su dimensión natural —ambigua, polisémica, indeterminada— como jurídica, con su pretensión de objetividad, pero sin escapar a la interpretación.

En tercer lugar, se expone cómo dichos sesgos son trasladados, replicados e incluso amplificados en los sistemas de inteligencia artificial, especialmente cuando se entrenan con datos generados por humanos. Finalmente, se ofrece una reflexión crítica sobre los límites y posibilidades de corregir o mitigar estos sesgos, proponiendo una mirada ética, normativa y estructural que supere la ilusión de neutralidad técnica.

II. Los sesgos cognitivos y su fundamento humano

i. Heurísticos y sesgos cognitivos: definición y relación

A. Definición

En la toma de decisiones humanas, los heurísticos se configuran como atajos mentales o estrategias cognitivas simplificadas, empleadas para emitir juicios con base en experiencias previas, sin necesidad de procesar exhaustivamente toda la información disponible. Como lo explica Nieva, un heurístico puede entenderse como una directriz general que orienta nuestras decisiones a partir del recuerdo de situaciones similares, replicando respuestas que resultaron eficaces en el pasado⁹.

Por su parte, los sesgos cognitivos representan “formas no razonadas en que se toman las decisiones, permitiendo hacer deducciones sin un alto nivel de esfuerzo, lo que podría desencadenar que la toma de decisiones sea tendenciosa o errada”¹⁰. Es decir, son distorsiones sistemáticas del pensamiento, producto de la aplicación no crítica de heurísticos en contextos que exigen mayor análisis o información.

B. Vinculación entre heurísticos y sesgos

A partir de los influyentes estudios de Tversky y Kahneman, se evidenció una relación intrínseca entre los heurísticos como mecanismos adaptativos de la cognición humana y los sesgos como consecuencias de su mal uso o aplicación automática¹¹. En palabras de Castro et al., cuando estos atajos mentales no conducen a una elección adecuada, dan lugar a sesgos cognitivos, generando decisiones basadas más en preconceptos internos y subjetivos que en razonamientos lógicos o normativos rigurosos¹².

⁹ NIEVA, J. (2018). Inteligencia artificial y proceso judicial. Marcial Pons.

¹⁰ CASTRO, A. et al. (2019). Nivel de sesgos cognitivos de representatividad y confirmación en estudiantes de Psicología de tres universidades del Bío-Bío. *Propósitos y Representaciones*, vol. 7, no. 2, pp. 210-239.

¹¹ TVERSKY, A. y KAHNEMAN, D. (1974). Judgment under Uncertainty: Heuristics and Biases. *Science*, vol. 185, no. 4157, pp. 1124-1131.

¹² CASTRO, A. et al. (2019). Nivel de sesgos cognitivos de representatividad y confirmación en estudiantes de Psicología de tres universidades del Bío-Bío. *Propósitos y Representaciones*, vol. 7, no. 2, pp. 210-239.

Desde esta perspectiva, es posible afirmar que los sesgos no son meros errores fortuitos, sino manifestaciones estructurales de los límites del juicio humano. Y, dado que la inteligencia artificial se construye precisamente sobre datos y patrones humanos, estos sesgos no desaparecen al ser informatizados, sino que son trasladados al sistema algorítmico, muchas veces con una potencia amplificadora.

ii. Impacto de los sesgos cognitivos en la toma de decisiones jurídicas

El ámbito jurídico no escapa a esta condición. Como señala Nieva, la actividad jurisdiccional, aunque formalmente guiada por la legalidad, está profundamente atravesada por atajos mentales, especialmente en contextos de alta carga procesal o presión institucional¹³. En tales escenarios, los jueces —como cualquier otro actor humano— recurren a heurísticos que, aunque útiles, pueden derivar en decisiones afectadas por sesgos cognitivos.

En primer lugar, el heurístico de representatividad se activa cuando se evalúa una situación según el grado de similitud con un modelo o categoría preexistente. Un juez, por ejemplo, puede asociar el caso presente con uno previo de características similares, y decidir conforme a su experiencia anterior, aun si los matices del nuevo caso requieren una valoración diferenciada. Este mismo mecanismo puede ser replicado por un sistema de IA, pero traducido en cálculos probabilísticos y patrones estadísticos¹⁴.

En segundo lugar, el heurístico de anclaje y ajuste se manifiesta cuando el juicio inicial se ve excesivamente condicionado por un valor de referencia, que no logra ser corregido de forma suficiente pese a la aparición de nueva información. Así, un magistrado podría establecer una pena inicial basada en precedentes jurídicos disímiles, y luego realizar ajustes menores que no alcanzan a corregir el error de origen. En contraposición, los sistemas algorítmicos tienden a modificar sus conclusiones únicamente cuando se reconfiguran los datos de entrada o se reentrena el modelo, lo que restringe su flexibilidad adaptativa en comparación con el juicio humano¹⁵.

¹³ NIEVA, J. (2018). *Inteligencia artificial y proceso judicial*. Marcial Pons.

¹⁴ *Idem*.

¹⁵ *Idem*.

No obstante, para comprender cabalmente el fenómeno de los sesgos, es necesario ampliar el análisis hacia su dimensión lingüística. En este sentido, la filosofía del lenguaje de Wittgenstein ofrece una base teórica fundamental: según su planteamiento, el lenguaje no es un espejo neutro de la realidad, sino una herramienta limitada que estructura nuestra forma de percibir y describir el mundo¹⁶. Para Wittgenstein, los significados no están dados de forma fija, sino que dependen del uso contextual del lenguaje, lo que introduce una indeterminación semántica inherente a toda comunicación.

Esta idea tiene profundas implicancias: el lenguaje condiciona el pensamiento, y por tanto, todo sistema de interpretación automatizada del mundo —como es el caso de un algoritmo jurídico que veremos más adelante— estará atravesado por las limitaciones y ambigüedades del lenguaje humano del cual se alimenta. Así, los sesgos no sólo derivan de procesos cognitivos individuales, sino también de las estructuras lingüísticas que organizan nuestra experiencia social y jurídica.

Por consiguiente, los sesgos de lenguaje —en línea con Wittgenstein— no son anomalías corregibles mediante ajustes técnicos, sino manifestaciones estructurales de un sistema simbólico que, por definición, excluye, simplifica y clasifica la realidad. Cuando los datos se procesan en modelos de inteligencia artificial, estas ambigüedades semánticas no desaparecen, sino que se traducen a otra lógica (la lógica computacional), que a su vez reproduce y refuerza ciertas formas de entender el mundo, muchas veces sin que sus supuestos sean explícitos o transparentes.

En suma, la toma de decisiones jurídicas está constantemente expuesta a sesgos cognitivos y lingüísticos que inciden tanto en la racionalidad de los jueces como en el diseño y funcionamiento de los sistemas judiciales. Reconocer esta doble dimensión es clave para evaluar críticamente el uso de la inteligencia artificial en el derecho, pues el riesgo no radica solo en la automatización de decisiones, sino en la automatización de prejuicios históricamente normalizados.

¹⁶ WITTGENSTEIN, L. (1922). *Tractatus logico-philosophicus*. Kegan Paul, Trench, Trubner & Co., LTD.

III. El lenguaje como núcleo del sesgo estructural

i. El lenguaje natural y sus sesgos: ambigüedad, indeterminación, interpretación

A. Imperfección del lenguaje humano

El lenguaje natural es inherentemente impreciso, ambiguo y contextual, lo cual permite la riqueza expresiva, pero también genera profundas dificultades cuando se pretende sistematizar o automatizar. Como señala Wittgenstein en sus *Investigaciones Filosóficas*, el significado de una palabra está en su uso dentro de un “juego de lenguaje”, es decir, es inseparable de sus contextos sociales e históricos¹⁷. Esta naturaleza flexible y polisémica del lenguaje humano entra en contradicción con los requerimientos de precisión y univocidad del lenguaje computacional.

En el campo de la inteligencia artificial, esta imprecisión se traduce en una tensión constante entre el lenguaje natural y el lenguaje formal. Los modelos computacionales que trabajan con procesamiento de lenguaje natural (NLP) —como GPT, Watson o Debater de IBM como veremos más adelante— intentan capturar patrones de uso y significado mediante estadísticas y redes neuronales, pero siempre con el riesgo de reproducir los sesgos sociales codificados en el corpus textual del cual se alimentan.

B. Sesgos semánticos y estructurales

Uno de los ejemplos más evidentes son los sesgos semánticos derivados de la polisemia y la ambigüedad léxica. Por ejemplo, la palabra “justicia” puede tener significados radicalmente distintos dependiendo del contexto (retributiva, distributiva, restaurativa), del hablante (juez, víctima, acusado) y del momento histórico (liberal, socialista, populista).

Asimismo, palabras como “violencia”, “autoridad” o “discriminación” no solo tienen múltiples sentidos, sino que esos sentidos están estructuralmente ligados a visiones ideológicas del mundo. Los modelos de IA, al ser entrenados con textos provenientes de medios

¹⁷ WITTGENSTEIN, L. (1999). *Investigaciones filosóficas*. Ediciones Altaya.

de comunicación, literatura jurídica, redes sociales o sentencias judiciales, aprenden esas correlaciones semánticas sin comprender su dimensión crítica, reproduciendo relaciones entre conceptos que pueden estar cargadas de prejuicios o suposiciones no verificadas.

Un ejemplo concreto es el de los embeddings de palabras utilizados por modelos como Word2Vec o GloVe: se ha comprobado que dichos modelos asocian términos como “hombre” con “ciencia” o “mujer” con “hogar” simplemente por la frecuencia estadística de esas relaciones en los textos analizados, lo cual reproduce estereotipos de género¹⁸.

ii. El lenguaje jurídico como convención estructurada (y su falibilidad)

A. Pretensión de objetividad en el derecho

El lenguaje jurídico ha sido históricamente construido como una convención institucionalizada orientada a dotar de certeza y previsibilidad a la aplicación del derecho. Para ello, recurre a mecanismos como la normatividad abstracta, las definiciones legales precisas, y el uso de técnicas interpretativas sistemáticas, que buscan reducir la ambigüedad propia del lenguaje natural. Esta arquitectura normativa permite hablar de una cierta pretensión de objetividad en el discurso jurídico, en la medida en que intenta garantizar condiciones mínimas de estabilidad semántica y control racional sobre el uso del poder público.

Sin embargo, esta pretensión es, en el fondo, parcial y falible. El derecho, en tanto fenómeno lingüístico y social, no escapa a la indeterminación estructural del lenguaje natural, tal como lo han

¹⁸ Véase BOLUKBASI, T., CHANG, K. W., ZOU, J. Y., SALIGRAMA, V., & KALAI, A. T. (2016). Man is to Computer Programmer as Woman is to Homemaker? Debiasing Word Embeddings. In *Advances in Neural Information Processing Systems*. NEURIPS (2016), CALISKAN, A., BRYSON, J. J., & NARAYANAN, A. (2017). Semantics derived automatically from language corpora contain human-like biases. *Science*, pp. 183–186.

advertido autores como Alexy¹⁹ y Ferrajoli²⁰. Este último afirma que el Derecho moderno es un “sistema de normas secundarias”, que pretende establecer reglas sobre cómo se crean, interpretan y corrigen otras normas. Pero incluso este metanivel normativo no elimina su condicionamiento ideológico, ni su dependencia de contextos históricos y estructuras de poder. La semántica jurídica, por tanto, no es neutral: está atravesada por conflictos interpretativos, disputas por el sentido, y tensiones entre el texto normativo y los valores constitucionales en juego.

Esto implica reconocer que el lenguaje jurídico, aunque aspire a la objetividad, funciona como una convención estructurada, pero abierta, en la cual las palabras no remiten de manera unívoca a significados fijos, sino que su sentido se configura discursivamente. En otras palabras, el lenguaje jurídico no puede ser reducido a un código cerrado, sino que opera como una práctica argumentativa institucionalizada, donde el significado es siempre el resultado de un proceso interpretativo.

B. Relación con la teoría de la argumentación jurídica

Frente a esta indeterminación, la teoría de la argumentación jurídica ha mostrado que el razonamiento jurídico no puede concebirse como una operación meramente lógica o deductiva, sino como una práctica racional discursiva, donde se busca justificar normativamente las decisiones jurídicas mediante argumentos plausibles, reconstruibles y contextualmente adecuados.

Autores como Perelman, Alexy y Atienza han desarrollado modelos teóricos que reconocen el carácter abierto del lenguaje jurídico y la necesidad de criterios de racionalidad práctica para orientarlo. En esta línea, Atienza²¹ sostiene que los enunciados jurídicos “no tienen un sentido fijo”, lo que obliga a que el jurista construya sentidos mediante operaciones interpretativas, analógicas y ponderativas, todo dentro de un marco institucional de justificación.

¹⁹ ALEXY, R. (2017). *Teoría de la argumentación jurídica: la teoría del discurso racional como teoría de la fundamentación jurídica*. Palestra Editores.

²⁰ FERRAJOLI, L. (2018). *Derecho y razón. Teoría del garantismo penal*. Trotta 10.^a ed.

²¹ ATIENZA, M. (2016). *Las razones del Derecho: Teorías de la argumentación jurídica* (Colección Derecho y Argumentación, cap. 1. Palestra Editores.

Por ejemplo, Alexy articula su propuesta sobre la base de una “lógica de la argumentación jurídica” que conjuga exigencias de coherencia formal con la inclusión de principios constitucionales y elementos del contexto práctico²². Así, el razonamiento jurídico implica juicios de valor estructurados racionalmente, donde el significado de las normas depende de su articulación con otras normas, principios y hechos del caso.

En consecuencia, cualquier intento de formalizar o automatizar el razonamiento jurídico –como pretenden ciertos modelos algorítmicos de inteligencia artificial– debe enfrentar necesariamente esta ambigüedad estructural del lenguaje jurídico. Esta ambigüedad no es un defecto, sino una condición inherente a su funcionamiento práctico, que habilita la interpretación y garantiza su adaptabilidad a contextos cambiantes, aunque también introduce zonas de disputa hermenéutica. En última instancia, lo que está en juego no es solo el significado de las palabras, sino la legitimidad racional del poder jurídico que las interpreta.

iii. El problema de la traducción al lenguaje de programación

A. De lo natural a lo formal

Uno de los mayores retos en la construcción de sistemas de inteligencia artificial jurídica es la traducción del lenguaje natural (o jurídico) al lenguaje de programación, es decir, a estructuras formales de datos, funciones y reglas lógicas. Esta traducción implica una pérdida inevitable de riqueza semántica y contexto. Como advierte Ashley²³, aunque es posible modelar ciertos elementos del razonamiento jurídico, los sistemas computacionales actuales aún enfrentan dificultades importantes para incorporar la indeterminación estructural del Derecho.

Por ejemplo, los estándares de prueba en derecho penal, como el de “más allá de toda duda razonable”, no son simplemente umbrales de probabilidad, sino juicios cualitativos que implican una convicción moral reforzada por la argumentación y el contexto. Como

²² ALEXY, R. (2017). *Teoría de la argumentación jurídica: la teoría del discurso racional como teoría de la fundamentación jurídica*. Palestra Editores.

²³ ASHLEY, K. (2023). *Inteligencia artificial y analítica jurídica: nuevas herramientas para la práctica del derecho en la era digital*. Yachay Legal.

señala Weiss²⁴, para que un sistema computacional evalúe si una afirmación satisface un estándar probatorio, debe tener acceso a los supuestos valorativos y fácticos que hacen aceptable una inferencia en una comunidad jurídica determinada, lo cual es extremadamente complejo de formalizar.

B. Pérdida de contexto y significado

La experiencia con programas como IBM Debater — como veremos más adelante — ha evidenciado esta dificultad. Aunque el sistema es capaz de detectar argumentos a favor y en contra de un tema específico, su evaluación depende de correlaciones textuales y no del contenido normativo o axiológico de los argumentos. Cuando Debater intentó analizar la constitucionalidad de una ley del Estado de California sobre videojuegos violentos, sus predicciones no lograron captar el estándar de escrutinio estricto aplicado por la Corte Suprema, ni los principios fundamentales en juego, como la libertad de expresión o el interés estatal en proteger a los menores.

Este tipo de errores no son meramente técnicos: son fallos epistémicos, que reflejan la imposibilidad de una equivalencia perfecta entre norma, hecho y código. La automatización de decisiones jurídicas implica no solo computar hechos, sino evaluar valores, contextos, trayectorias jurisprudenciales y sentidos comunes jurídicos — todo lo cual es muy difícil de codificar sin perder la riqueza del lenguaje jurídico —.

IV. Los sesgos en la inteligencia artificial y en los algoritmos

i. Herencia humana: cómo se trasladan los sesgos a los sistemas

A. Programación realizada por humanos

Una de las características estructurales más importantes de la inteligencia artificial (IA) radica en que los algoritmos son diseñados por humanos y se entrenan con datos generados por humanos, lo cual implica que no son neutros ni imparciales por defecto. Desde una perspectiva epistemológica, esto significa que **los sesgos**

²⁴ WEISS, C. (2003). "Expressing Scientific Uncertainty." *Law, Probability and Risk*, pp. 25-46.

cognitivos, sociales y lingüísticos de quienes diseñan y entrenan los sistemas pueden replicarse —consciente o inconscientemente— en el comportamiento de la IA.

De acuerdo con Ashley, los primeros sistemas legales expertos, como WLES (Waterman Legal Expert System) o Taxman II, ya enfrentaban limitaciones estructurales derivadas de su dependencia del lenguaje jurídico, las reglas heurísticas y el razonamiento por encadenamiento (forward o backward chaining)²⁵. Estos sistemas, aunque sofisticados para su época, se basaban en marcos conceptuales previamente definidos por humanos, lo cual conllevaba el riesgo de reproducir concepciones jurídicas sesgadas o parciales, dependiendo del contexto doctrinal, jurisprudencial o ideológico del programador.

B. Reproducción de los sesgos en los sistemas

Pese a la creencia popular, los sistemas de inteligencia artificial no están exentos de sesgos, sino que más bien los heredan estructuralmente de los humanos, quienes programan su funcionamiento y proveen sus datos de entrenamiento²⁶. Al respecto, Irazabal advierte que “no se trata de un error que pueda evitarse, sino de una condición esencial para el conocimiento de cualquier tipo”²⁷. A partir de ello, es posible afirmar que la presencia misma del sesgo no implica necesariamente una falla, pero sí una alerta epistémica que requiere ser gestionada con rigurosidad para evitar su propagación acrítica en sistemas automatizados.

Un estudio empírico reveló que la ausencia de identificación y corrección de estos sesgos no solo afecta la efectividad en la toma de decisiones, sino que además puede producir una “herencia de sesgo”²⁸. Es decir, los usuarios que interactúan con sistemas

²⁵ ASHLEY, K. (2023). Inteligencia artificial y analítica jurídica: nuevas herramientas para la práctica del derecho en la era digital. Yachay Legal.

²⁶ VICENTE, L. & MATUTE, H. (2023). Humans inherit artificial intelligence biases. *Scientific Reports*.

²⁷ IRAZABAL, E. (2023). La Inteligencia Artificial explicada para abogados. La Ley.

²⁸ VICENTE, L. & MATUTE, H. (2023). Humans inherit artificial intelligence biases. *Scientific Reports*.

sesgados tienden a internalizar dichos sesgos y a reproducirlos en decisiones futuras, incluso después de haber cesado el uso del sistema²⁹, lo que genera un círculo vicioso de decisiones erradas amplificadas tecnológicamente.

Este problema no es meramente técnico, sino profundamente lingüístico y filosófico. Desde la perspectiva del lenguaje de Wittgenstein como de Saussure, es posible comprender que el significado de una palabra está determinado por su uso en un juego de lenguaje específico, y que el lenguaje es, en última instancia, una forma de vida. Esto implica que las resoluciones judiciales, al ser textos jurídicos cargados de significado, no son estructuras objetivas e inmutables, sino expresiones de contextos culturales, institucionales e históricos específicos. De este modo, las ambigüedades, indeterminaciones semánticas y disputas conceptuales propias del Derecho también son transferidas a los sistemas de IA cuando estos se entrenan con textos jurídicos.

Ashley advierte que muchos programas actuales, como Ravel, Lex Machina o Ross Intelligence, aunque utilizan técnicas sofisticadas de analítica textual, no superan del todo el problema del sesgo semántico, pues analizan el lenguaje normativo desde sus representaciones textuales, pero sin comprender su complejidad pragmática o filosófica³⁰. En efecto, estos programas tienden a tratar los signos jurídicos como estructuras cerradas, pero ignoran que, como señala Wittgenstein en el fundamento 43 de su *Tractatus*³¹, “el significado de una palabra es su uso en el lenguaje”, lo que en el campo jurídico se traduce en que el mismo término puede adoptar sentidos distintos según el foro, el juez, la doctrina dominante o el contexto fáctico.

²⁹ VIDAL, G. (2008). “La teoría de la elección racional en las ciencias sociales”, *Revista Sociológica*, pp. 12.

³⁰ ASHLEY, K. (2023). Inteligencia artificial y analítica jurídica: nuevas herramientas para la práctica del derecho en la era digital. Yachay Legal.

³¹ WITTGENSTEIN, L. *Tractatus Logico-Philosophicus*. Escuela de Filosofía Universidad ARCIS, fundamento 43.

Por ejemplo, Ashley menciona que algunos programas entrenados con decisiones judiciales (case-based reasoning systems) funcionan a partir de modelos previos que pueden no ser representativos de la totalidad del derecho vigente, o incluso pueden haberse basado en sentencias controvertidas, inexactas o inestables³². Esto evidencia que la base sobre la cual se entrena la IA jurídica es epistemológicamente frágil. Si a esto se suma que el programador puede incorporar —de forma deliberada o accidental— determinados intereses, paradigmas o limitaciones culturales, entonces el sistema deja de ser una herramienta imparcial para convertirse en un mecanismo de reproducción de sesgos estructurales, incluso ideológicos.

Este escenario exige una reflexión crítica: si la inteligencia artificial depende de datos y estructuras lingüísticas que son construidas, discutidas y disputadas socialmente, entonces su desarrollo ético y técnico no puede desentenderse de una concepción filosófica del lenguaje y del conocimiento. Solo reconociendo la fragilidad epistémica del lenguaje jurídico, su ambigüedad semántica y su carácter disputable, es posible diseñar sistemas que no perpetúen ciegamente los sesgos humanos, sino que los enfrenten desde una lógica reflexiva y autocrítica.

ii. Casos ilustrativos: Compass, IBM Debater, entre otros

A. Sistema COMPAS (EE.UU.)

El sistema COMPAS (Correctional Offender Management Profiling for Alternative Sanctions), desarrollado por Northpointe (actualmente Equivant), es un instrumento de evaluación de riesgos de cuarta generación que se aplica en diversas etapas del proceso penal, particularmente en decisiones de libertad condicional y sentencias. Según su propia “Guía para profesionales”, busca identificar necesidades criminógenas y riesgos de reincidencia, a través del análisis de más de 137 variables³³.

³² ASHLEY, K. (2023). Inteligencia artificial y analítica jurídica: nuevas herramientas para la práctica del derecho en la era digital. Yachay Legal.

³³ NORTHPOINTE. (2015). Practitioner’s Guide to COMPAS Core.

No obstante, este procesamiento de datos no escapa a condicionamientos estructurales: si las variables utilizadas están impregnadas por desigualdades históricas —como antecedentes policiales desproporcionadamente altos en comunidades racializadas, o factores socioeconómicos interpretados como indicadores de riesgo³⁴—, el sistema no solo reproduce, sino que automatiza la discriminación. En ese sentido, el sesgo no es una mera falla técnica, sino una manifestación algorítmica de asimetrías sociales preexistentes. El riesgo radica en que, al integrarse en decisiones judiciales con efectos jurídicos, estos sesgos adquieren un carácter normativo, institucionalizando la exclusión bajo el manto de una supuesta neutralidad técnica.

Esta institucionalización ocurre cuando los resultados sesgados del sistema se convierten en insumos regulares para decisiones formales (libertad condicional, medidas cautelares, sentencias), sin que se visibilice su origen desigual o se activen mecanismos de corrección³⁵. Así, lo que debería ser un instrumento auxiliar se transforma en una fuente de legitimación de prácticas discriminatorias, blindadas por el prestigio del dato y la opacidad del algoritmo.

Investigaciones como la de Roa et al. (2022) y reportes de ProPublica han evidenciado cómo este sistema, lejos de garantizar neutralidad, reproduce y amplifica sesgos raciales, otorgando mayores puntajes de riesgo a personas afrodescendientes en comparación con personas blancas en condiciones similares³⁶. Esto evidencia un problema estructural: la IA jurídica puede institucionalizar la discriminación preexistente bajo un barniz técnico de objetividad.

³⁴ FIGUEROA, M., REBOLLEDO, R. (2024). Presentación Dossier. Racismos. Ideología del mestizaje y colonialismo. Reflexiones para repensar los procesos de alterización de nuestra América. CUHSO (Temuco), vol. 34, no. 2.

³⁵ *Idem*.

³⁶ ROA, M.; SANABRIA, J.; DINAS, K. (2022). Uso del algoritmo COMPAS en el proceso penal y los riesgos a los derechos humanos. *Rev. Bras. De Direito Processual Penal*, vol. 8, no. 1, pp. 275-310.

B. IBM Debater y los límites del lenguaje argumentativo

Un caso más sofisticado es IBM Project Debater, sucesor del célebre Watson. Este sistema, probado públicamente en 2014, fue diseñado para participar en debates complejos sobre cuestiones sociales. Al ser presentado con un tópico —por ejemplo, “¿Debería prohibirse la venta de videojuegos violentos a menores?”—, escaneó millones de fuentes, seleccionó los argumentos relevantes, los clasificó como favorables o contrarios, y construyó un esquema discursivo automatizado.

Este experimento, estudiado por Dvorsky³⁷ y comentado por Ashley, muestra los alcances de la minería de argumentación automatizada, pero también sus limitaciones: el sistema fundamentó su argumento en una interpretación literal del Código Civil de California y del caso *Brown v. Entertainment Merchants Association*, sin captar que la resolución del tribunal supremo estadounidense no sólo evaluó la norma, sino que aplicó un test de escrutinio estricto basado en principios constitucionales más complejos (Primera y Decimocuarta Enmienda).

Esto revela un hecho crucial: la argumentación jurídica no se agota en el análisis textual ni lógico-formal, sino que requiere una ponderación de valores, contextos y principios que los sistemas computacionales actuales aún no pueden reproducir con fidelidad. Como afirma Ashley, los modelos computacionales deben incorporar estándares de prueba bien definidos, tales como el más allá de toda duda razonable, para que una conclusión jurídica sea aceptable dentro del sistema³⁸.

C. Reflexión crítica

La cuestión central es entonces: *¿puede la IA juzgar con mayor objetividad que un humano? ¿O simplemente reproduce, con mayor velocidad, los mismos sesgos del lenguaje y los datos humanos?* En efecto, los modelos de IA —por más avanzados que sean— se alimentan

³⁷ DVORSKY, G. (2014, May 5). IBM's Watson Can Now Debate Its Opponents (minute 45:47). Gizmodo, (Consultado el 13 de mayo del 2025).

³⁸ ASHLEY, K. (2023). Inteligencia artificial y analítica jurídica: nuevas herramientas para la práctica del derecho en la era digital. Yachay Legal.

de corpus lingüísticos, decisiones previas y datos históricos, todos ellos atravesados por visiones ideológicas, valores implícitos y estructuras de poder.

Además, como bien advierte Ashley, los sistemas jurídicos no son homogéneos ni políticamente neutros³⁹. Existen sistemas como el estadounidense, fuertemente influido por precedentes y razones institucionalizadas (“institutional reasons”), y otros como el continental europeo o el peruano, donde el formalismo legal convive con una fuerte influencia política, mediática y cultural. En consecuencia, pretender que una IA pueda abstraerse de este contexto es desconocer la naturaleza política del derecho.

Sin embargo, el problema no radica únicamente en la reproducción de sesgos humanos por parte de la IA, sino en su amplificación y normalización bajo una apariencia de objetividad algorítmica, así propiciando una discriminación institucional. Esto ocurre, por ejemplo, con el sistema COMPAS, diseñado para estimar el riesgo de reincidencia en el proceso penal estadounidense, el cual ha sido criticado por su falta de transparencia y por reproducir sesgos raciales preexistentes⁴⁰.

Sobre este punto, resulta pertinente analizar la incidencia del sesgo de representatividad, el cual se manifiesta cuando COMPAS, alimentado con datos históricos del sistema de justicia penal que ya habían adquirido sesgos contra ciertas minorías, construye un “prototipo” de alto riesgo, lo que deriva en puntuaciones artificialmente infladas para individuos pertenecientes a tales minorías, al basar su análisis en estadísticas grupales más que en el riesgo individual⁴¹. De manera análoga, el sesgo de anclaje y ajuste opera cuando las minorías son objeto de un número mayor de detenciones, siendo que estas anclas las sitúan, desde el

³⁹ *Idem.*

⁴⁰ ARIZA, J. (2022). Inteligencia artificial legal y administración de justicia. En S. Calaza y M. Sánchez-Arjona (Dir.), *Impugnación de las decisiones judiciales dictadas con auxilio de inteligencia artificial*, pp. 29-54. Thomson Reuters Aranzadi.

⁴¹ ROA, M.; SANABRIA, J.; DINAS, K. (2022). Uso del algoritmo COMPAS en el proceso penal y los riesgos a los derechos humanos. *Rev. Bras. De Direito Processual Penal*, vol. 8, no. 1, pp. 275-310.

principio, en un perfil de riesgo elevado que ajustes posteriores no logran compensar. De ahí que, la aplicación institucional de estas puntuaciones viciadas por los sesgos perpetúa la discriminación en el sistema judicial, siendo un factor agravante la “caja negra” intrínseca a los algoritmos que obstaculiza la auditoría de sus procesos y, en consecuencia, la rendición de cuentas⁴².

Ahora bien, lo más inquietante no es, en realidad, que la inteligencia artificial o los algoritmos puedan equivocarse, sino que estos sesgos sean automatizados y consolidados por las instituciones que debieran impartir justicia. Este fenómeno, además de comprometer una evaluación objetiva y amenazar la salvaguarda de principios como el debido proceso y la no discriminación⁴³, revela el desafío que enfrenta el Derecho en su propia digitalización: el de no ceder de su rol garantista frente a herramientas que transforman sesgos en decisiones judiciales con apariencia de objetividad.

iii. Mecanismos actuales de detección y corrección (y sus limitaciones)

A. Técnicas para mitigar sesgos

Frente al creciente reconocimiento de los sesgos estructurales que afectan a los sistemas de inteligencia artificial (IA) jurídica, se han desarrollado múltiples estrategias tanto técnicas como institucionales para su identificación, mitigación y posible corrección. Estas soluciones buscan reducir el impacto discriminatorio que pueden tener las decisiones automatizadas, sobre todo en contextos de alta sensibilidad como el penal o el constitucional.

Entre los mecanismos más utilizados destacan:

- a. **Preprocesamiento de datos (data cleansing):** Consiste en la eliminación o anonimización de variables sensibles (como raza, género o lugar de residencia), así como en la corrección de desbalances en los conjuntos de datos. Sin embargo, esta técnica

⁴² MIRÓ, F. (2018). Inteligencia artificial y justicia penal: más allá de los resultados lesivos causados por robots. UNED, vol. 3, no. 20, pp. 87-130.

⁴³ ROA, M.; SANABRIA, J.; DINAS, K. (2022). Uso del algoritmo COMPAS en el proceso penal y los riesgos a los derechos humanos. Rev. Bras. De Direito Processual Penal, vol. 8, no. 1, pp. 275-310.

ha sido cuestionada por su superficialidad, ya que borrar datos sensibles no impide que correlaciones indirectas (proxies) reproduzcan los mismos sesgos.

- b. Auditorías algorítmicas externas e independientes:** Evaluaciones sistemáticas, realizadas por terceros imparciales, que buscan examinar la equidad y transparencia de un modelo en diferentes escenarios. A menudo se emplean metodologías como pruebas de caja negra o análisis contrafactuales para determinar si un sistema responde de forma desigual ante casos similares.
- c. Métricas de justicia algorítmica (*fairness metrics*):** Criterios cuantitativos que permiten evaluar si un algoritmo respeta ciertos principios normativos. Entre ellos se encuentran el demographic parity (paridad demográfica), equality of opportunity (igualdad de oportunidades) y disparate impact (impacto adverso). Estas métricas buscan formalizar, dentro del lenguaje técnico, intuiciones legales sobre discriminación y trato desigual.
- d. Técnicas de aprendizaje adversarial y regularización:** Estas estrategias se centran en entrenar al sistema para que no se sobreajuste a patrones sesgados presentes en los datos. Por ejemplo, se introduce un “adversario” que intenta identificar sesgos en las predicciones del modelo, forzándolo a generalizar mejor.

Pese al avance técnico, estas medidas enfrentan limitaciones conceptuales y prácticas cuando se insertan en sistemas jurídicos complejos, políticamente definidos y normativamente conflictivos.

B. Críticas y limitaciones

A pesar de los esfuerzos descritos, existe un consenso creciente en la literatura crítica sobre los límites estructurales e inherentes de estas soluciones técnicas. Como advierte Roa (2022), no es posible “limpiar” un conjunto de datos que ya refleja un mundo desigual: el sesgo no es simplemente un error técnico corregible, sino una expresión profunda de la cultura, el lenguaje y la estructura del poder en el derecho⁴⁴.

⁴⁴ *Idem.*

Desde esta perspectiva, el problema no radica solamente en cómo se entrena un algoritmo, sino en **qué tipo de sistema jurídico y político** da origen a los datos y qué valores se privilegian al automatizar sus decisiones. Tal como lo señala Ferrajoli, el derecho no es un sistema neutro, sino el resultado de luchas históricas, conflictos sociales y estructuras de poder⁴⁵. Así, la IA jurídica no puede ser comprendida únicamente como una herramienta técnica, sino como un nuevo campo de disputa por la definición misma de lo justo y lo injusto, incluso también del aun extenuante debate de lo verdadero o falso de Bruno Cavallone y Michelle Taruffo⁴⁶.

Este enfoque cobra especial relevancia en contextos como el peruano del año 2025, caracterizado por una débil institucionalidad, alta volatilidad normativa y fuerte instrumentalización política del derecho. En tales condiciones, la pretensión de construir una IA jurídica objetiva se convierte en una empresa epistemológicamente inviable y políticamente riesgosa. Automatizar decisiones jurídicas justas presupone, al menos, la existencia de un sistema normativo estable, coherente y legítimo, condición que hoy no se cumple. De lo contrario, el riesgo no es solo replicar sesgos individuales, sino institucionalizar sesgos estructurales bajo el ropaje de la neutralidad algorítmica, sin ningún control democrático ni mecanismos efectivos de rendición de cuentas.

C. Estándares de prueba y modelos computacionales de argumentación jurídica

En los modelos computacionales de argumentación jurídica, los estándares de prueba constituyen un pilar esencial para estructurar razonamientos válidos y aceptables. Como ha señalado Weiss⁴⁷, estos estándares no solo orientan la toma de decisiones, sino que también permiten que las máquinas evalúen cuándo una afirmación

⁴⁵ FERRAJOLI, L. (2018). *Derecho y razón. Teoría del garantismo penal*. Trotta 10.^a ed.

⁴⁶ CAVALLONE, B. y TARUFFO, M. (2012). *Un diálogo sobre prueba y verdad* (Colección Palestra Extramuros). Lima: Editorial Palestra.

⁴⁷ WEISS, C. (2003). *Expressing Scientific Uncertainty. Law, Probability and Risk*, vol. 2, pp. 25-46.

jurídica ha alcanzado un umbral probatorio determinado, como ocurre con el clásico “más allá de toda duda razonable” en el proceso penal.

En esa línea, Weiss indica que, para que un sistema de IA jurídica emule una decisión humana válida, debe incorporar estándares que funcionen como metas evaluables, es decir, niveles mínimos de aceptabilidad para que una afirmación sea tomada en cuenta. Este principio permite que las máquinas no solo acumulen datos, sino que razonen con base en reglas definidas, construyendo convicciones firmes y excluyendo decisiones con márgenes inaceptables de incertidumbre.

Un ejemplo paradigmático de los desafíos que enfrentan estos sistemas lo representa IBM Debater, descendiente del famoso Watson. En 2014, IBM probó un sistema capaz de escanear millones de textos (como Wikipedia) y generar argumentos a favor y en contra de una proposición, tal como “la venta de videojuegos violentos a menores debería estar prohibida”⁴⁸. Para ello, el sistema analizó más de 4 millones de artículos, extrajo oraciones relevantes, identificó alegatos, evaluó su polaridad y construyó una maqueta argumentativa.

No obstante, su razonamiento automatizado presentó fallos significativos cuando se comparó con casos reales, como *Video Software Dealers Association v. Schwarzenegger*, en el que la Corte Suprema de EE. UU. aplicó el escrutinio estricto sobre una ley californiana similar. IBM Debater no pudo captar que el valor constitucional de la libertad de expresión pesa más que el supuesto interés estatal en prohibir tales ventas. El problema de fondo fue que el sistema no comprendía la técnica de la ponderación —elemento que aún es discutible por su indefinición pragmatodialectica⁴⁹—, central en los modelos de argumentación jurídica compleja, donde los derechos y principios deben ser equilibrados con sensibilidad al contexto.

⁴⁸ ASHLEY, K. (2023). *Inteligencia artificial y analítica jurídica: nuevas herramientas para la práctica del derecho en la era digital*. Yachay Legal, pp. 61.

⁴⁹ VAN EEMEREN, F. (2019). *La teoría de la argumentación: Una perspectiva pragmatodialectica*. (Cap. 6, pp. 139-166) Palestra.

D. La cognición jurídica artificial y sus dilemas políticos

En años recientes, han surgido nuevas aplicaciones cognitivas jurídicas —como Ross, Lex Machina y Ravel— que no solo procesan normas, sino que evalúan contextos fácticos y jurisprudenciales. Estas herramientas buscan superar los límites del análisis meramente textual, incorporando elementos como tendencias jurisprudenciales, patrones estadísticos y lenguaje natural. Sin embargo, esta aparente sofisticación no elimina un problema central: la inclinación política y valorativa del derecho.

Según Atienza, citado por Summers, el sistema norteamericano —basado en “razones buenas” y no en pruebas racionales estructuradas— responde más a una tradición judicial que a un método lógico-deductivo⁵⁰. En cambio, los sistemas continentales, como el europeo, adoptan una estructura racional más definida. El Perú, sin embargo, representa una excepción sui generis: su sistema legal es fragmentario, ambiguo, inestable y permeable a intereses políticos, económicos y mediáticos.

Este contexto vuelve particularmente problemática cualquier tentativa de automatización jurídica. Como bien señala Ferrajoli, todo sistema de derecho refleja una visión política del mundo⁵¹; por tanto, automatizar decisiones sin definir previamente cuál visión política se implementa es equivalente a delegar a la máquina una función soberana sin legitimidad. De la misma manera, en la estructura de la argumentación jurídica, García destaca la importancia primaria de definir los patrones de significado y los parámetros de evaluación de los conceptos a utilizar en un sistema, cual se constituye en el concepto de “Tópica Jurídica”⁵².

En resumen, la inteligencia artificial jurídica no puede ser comprendida ni utilizada como una herramienta puramente técnica. Requiere de una estructura normativa definida, una ética jurídica consensuada y mecanismos de control institucional. Sin estos elementos, corre el riesgo de convertirse no en una lo aliada de

⁵⁰ SUMMERS, R. (2020). Las razones sustantivas y la interpretación del Derecho en el common law. Palestra Editores, p. 37.

⁵¹ FERRAJOLI, L. (2018). Derecho y razón. Teoría del garantismo penal. Trotta 10.^a ed.

⁵² GARCÍA, J. (2018). Teorías de la tópica jurídica. Palestra Editores.

la justicia, sino en una forma tecnocrática de reproducción de injusticias estructurales.

V. Conclusiones

- El lenguaje natural está dotado de ambigüedad e imprecisión, dependiendo de factores como el contexto y momento histórico en que se comunica un mensaje para lograr su correcta interpretación. El lenguaje jurídico no es la excepción, pues, aunque se utilicen diversas técnicas para atribuir objetividad y determinación al derecho, el entendimiento pleno de las ideas en el plano jurídico sigue estando supeditado a circunstancias propias de la realidad contemporánea. Por tales razones, para automatizar el razonamiento jurídico, se deberá abordar minuciosamente la ambigüedad estructural del lenguaje jurídico, a fin de procurar la mayor claridad posible en el uso de los sistemas de inteligencia artificial.
- Los heurísticos son estrategias cognitivas empleadas para simplificar el proceso de toma de decisiones; su aplicación debe reservarse a situaciones que no ameriten un análisis crítico o en profundidad. Cuando se utilizan indistintamente, devienen en sesgos (tanto estructurales o semánticos, como intencionales o funcionales), los cuales impiden el razonamiento lógico y objetivo que se esperaría de un sistema automatizado.
- Los sesgos son inherentes a la inteligencia artificial, dada la inevitabilidad de que sean heredados durante la programación de algoritmos. En ese orden de ideas, se han desarrollado diversos mecanismos de detección y corrección, cuyo fin es disminuir los efectos discriminatorios de los sesgos en los sistemas de inteligencia artificial jurídica. No obstante, su falta de eficacia indica que la IA no puede abstraerse completamente de los sesgos, en tanto que estos son manifestaciones de aspectos culturales, lingüísticos y políticos de una sociedad.
- En resumen, la inteligencia artificial jurídica no puede ser comprendida ni utilizada como una herramienta puramente técnica. Requiere de una estructura normativa definida, una ética jurídica consensuada y mecanismos de control institucional. Sin estos elementos, corre el riesgo de convertirse no en una aliada de la justicia, sino en una forma tecnocrática de reproducción de injusticias estructurales.

Protección de derechos fundamentales frente a nuevas tecnologías: estudio comparado de Chile, México, Colombia, Ecuador, Bolivia y Perú

Eduardo Chocano Ravina* y Lizty Maryel Obando Guerrero**

Resumen.- Este artículo analiza cómo los Estados constitucionales latinoamericanos han integrado las nuevas tecnologías y su impacto en los derechos fundamentales. Se examinan países como Chile, México, Colombia, Ecuador, Bolivia y Perú, y se propone un modelo de gobernanza tecnológica basado en los derechos humanos, que combine estabilidad normativa y flexibilidad interpretativa ante los avances tecnológicos.

Palabras Clave.- Tecnologías - Derechos fundamentales - Estado Constitucional.

Abstract.- This article examines how Latin American constitutional states have integrated new technologies and their impact on fundamental rights. It looks at countries like Chile, Mexico, Colombia, Ecuador, Bolivia, and Peru, proposing a human rights-based model of technological governance that combines regulatory stability and interpretive flexibility in response to technological advances.

Keywords.- Technologies - Fundamental Rights - Constitutional State.

* Bachiller de Derecho en la Universidad de Lima y estudiante de Filosofía en la Universidad TECH. Autor y coautor de artículos en derecho constitucional y las nuevas tecnologías. Columnista sobre política, realidad nacional, derecho y temas culturales.

** Egresada de Derecho en la Universidad Tecnológica del Perú. Ha participado en la elaboración de artículos académicos y ponencias centradas en justicia, derechos humanos y sistemas jurídicos comparados. Realizó una pasantía en la Corte Interamericana de Derechos Humanos.

I. Introducción

La acelerada expansión de las nuevas tecnologías ha modificado de manera profunda la forma en que las personas interactúan entre sí y con las instituciones del Estado. Este fenómeno genera oportunidades para el ejercicio y la protección de derechos. Empero, también plantea riesgos significativos que requieren respuestas jurídicas sólidas. A su vez, la creciente presencia de entornos digitales, inteligencia artificial, neurotecnologías y sistemas de vigilancia pone a prueba la capacidad de los ordenamientos constitucionales para garantizar la protección efectiva de los derechos fundamentales, particularmente la dignidad humana, la privacidad, la igualdad y la libertad.

En este contexto, América Latina constituye un laboratorio jurídico de especial interés, dada la coexistencia de marcos normativos heterogéneos y dinámicas institucionales diversas. Algunos Estados optaron por introducir disposiciones expresas en sus constituciones para atender los desafíos tecnológicos, mientras que otros han desarrollado soluciones principalmente a través de la jurisprudencia constitucional. Este artículo analiza de manera comparada las respuestas de Chile, México, Colombia, Ecuador, Bolivia y Perú. Estos países fueron seleccionados por tres criterios: (i) su cercanía geográfica y la existencia en cada una de ellas de una Constitución, (ii) la existencia de reformas constitucionales o decisiones judiciales recientes y de impacto, y (iii) la accesibilidad y disponibilidad de sus fuentes normativas para la investigación. La hipótesis que guía este estudio es que la incorporación de disposiciones constitucionales específicas ofrece mayores garantías de protección de derechos fundamentales frente a los riesgos de las nuevas tecnologías que las soluciones exclusivamente jurisprudenciales o de rango legal.

A su vez, la metodología se basa en un análisis comparado de fuentes primarias. En el caso de Chile, se estudia el texto constitucional reformado que introduce la protección de los denominados neuroderechos, constituyendo un precedente singular en la región. En los demás países, el examen se centra en la jurisprudencia de sus tribunales, cuyas decisiones han configurado criterios interpretativos frente a conflictos originados por el uso de tecnologías emergentes, en ausencia de reformas constitucionales específicas, como en la producción de rango legal.

Este enfoque permitió identificar con mayor precisión los avances, limitaciones y tensiones derivadas de cada modelo, así como las tendencias

comunes y vacíos normativos que inciden en la gobernanza tecnológica regional. Desde una perspectiva crítica, se argumenta que las respuestas constitucionales o jurisprudenciales a los desafíos tecnológicos deben construirse sobre principios claros y coherentes, capaces de equilibrar innovación y derechos fundamentales. La reflexión final apunta a que solo mediante un marco normativo sólido, con fundamentos en los valores esenciales del Estado constitucional, será posible garantizar que el desarrollo tecnológico se oriente al fortalecimiento de la dignidad humana, la equidad y la justicia.

II. Importancia de una Constitución para un Estado

Antes de analizar la inclusión de las nuevas tecnologías en las Constituciones latinoamericanas, es fundamental comprender el papel crucial que desempeña la Constitución en el marco del Estado. En este sentido, cabe destacar que existen diversas interpretaciones sobre el concepto de Constitución, por lo que resulta pertinente revisar las definiciones propuestas por destacados juristas, tanto clásicos como contemporáneos, de tradición nacional e internacional.

Uno de los aportes más influyentes en esta materia proviene de Hans Kelsen, jurista y filósofo austríaco, cuya obra sobre el control jurisdiccional de la constitucionalidad se ha convertido en una referencia obligatoria. Para Kelsen, la Constitución es concebida como:

[...] la idea de un principio supremo que determina por entero el orden estatal y la esencia de la comunidad constituida por ese orden. Como quiera que se defina, la Constitución es siempre el fundamento del Estado, la base del orden jurídico que se pretende conocer (1994, p.21)¹.

Asimismo, Bruce Ackerman, jurista estadounidense, destacó en su notable libro *We the People* (1991) que “la Constitución es primero democrática y, en segundo lugar, protectora de derechos”, ya que “la protección judicial de los derechos depende de una afirmación democrática previa” (citado por Ruiz, 2020, p.82)². A esta visión puede añadirse la perspectiva de Ronald Dworkin, quien considera que una Constitución debe ser

¹ KELSEN, H. (1994). La garantía jurisdiccional de la Constitución. La Justicia constitucional. *IUS ET VERITAS*, 5(9), pp. 17-43.

² RUIZ, C. (2020). Democracia y constitución. *Revista De La Academia*, (29), pp. 81-89.

interpretada a la luz de los principios morales que mejor justifican las prácticas jurídicas de una comunidad, enfatizando su rol como carta de derechos y como límite al poder político (citado por Lifante, 1999, pp. 43-44)³.

En el ámbito latinoamericano, se encuentran valiosas contribuciones que contextualizan la función constitucional dentro de las realidades nacionales. Por ejemplo, Aníbal Quiroga León, jurista peruano, la define como la máxima instancia del ordenamiento jurídico, actuando también como una norma política que engloba los principios y fundamentos clave para la organización política, social y económica de la nación (1985)⁴.

A su vez, Humberto Nogueira Alcalá, jurista y escritor constitucionalista chileno, sostiene que la existencia de una Constitución responde a una determinada concepción del orden político que se busca racionalizar y estructurar para lograr el correcto funcionamiento del Estado conforme a un modelo normativo legitimado (1993)⁵. En una línea similar, el jurista español Manuel Atienza, apoyándose en las ideas de Bovero, indica que la Constitución puede entenderse en dos sentidos: uno amplio, que refiere a la estructura y organización del poder en un Estado; y otro estricto y contemporáneo, que se refiere a una declaración de derechos fundamentales y un diseño institucional basado en la separación de poderes, propios del Estado constitucional de derecho (2007)⁶.

Por su parte, Raúl Chanamé Orbe, jurista peruano, plantea que la Constitución es el marco normativo fundamental desde el cual se regula la relación entre los ciudadanos y los poderes públicos. Además, sostiene que el control ejercido por la Constitución debe adecuarse a la realidad política, social, económica y cultural contemporánea, guiado por principios orientados a garantizar la máxima protección de la persona

³ LIFANTE, I. (1999). La teoría de Ronald Dworkin, la reconstrucción del derecho a partir de casos. *Jueces para la democracia*, 36, pp. 41-46.

⁴ Quiroga León, A. (1985). La interpretación constitucional. *Derecho PUCP*, (39), pp. 323-343.

⁵ NOGUEIRA, H. (2024). La justicia constitucional como defensa de la Constitución. *Revista Chilena De Derecho*, 20(2 y 3), pp. 417-439.

⁶ ATIENZA, M. (2007). Constitución y argumentación. *Anuario De Filosofía Del Derecho*, (24), pp. 197-228.

humana, reconocida como titular de derechos y portadora de un valor axiológico intrínseco denominado dignidad (2015)⁷.

Esta función dual de la Constitución, como norma jurídica suprema y como proyecto político fundacional, es también destacada por autores como César Castillo Córdova, quien afirma que la Constitución, en sus múltiples formas de comprensión, constituye una manifestación normativa destinada a regular de manera efectiva las relaciones entre ciudadanos y poder político, así como entre particulares (2005)⁸. De modo complementario, para Blancas Bustamante, la Constitución organiza tanto al Estado como el desarrollo de la vida de la población en su relación con este y con los demás miembros de la sociedad (2017)⁹.

En síntesis, los autores citados permiten comprender que la Constitución no solo cumple una función jurídica al estructurar el poder estatal, sino también una función política orientada a garantizar principios fundamentales como la dignidad humana. En tal sentido, al ser la norma suprema del ordenamiento, la Constitución organiza la vida en sociedad y establece los parámetros para las relaciones entre el Estado y los ciudadanos, lo que justifica plenamente su análisis en el contexto de los desafíos que imponen las nuevas tecnologías.

i. Adaptación de la Constitución a los cambios sociales

La Constitución, fundamento de la organización estatal, debe ajustarse a las transformaciones sociales para conservar vigencia y sintonía con la realidad; de ahí la idea de una Constitución viva, dinámica y en permanente construcción que expresa la identidad y el desarrollo cultural de la comunidad (Pomareda Muñoz, 2021)¹⁰. Para ello operan, principalmente, la reforma constitucional, que actualiza el texto para incorporar derechos emergentes, reordenar competencias o responder a

⁷ CHANAMÉ, R. (2015). *La Constitución Comentada* (Vol. 1, 1ª ed.). Lima: Ediciones Legales E.I.R.L.

⁸ Castillo, L. (2005). El carácter normativo fundamental de la Constitución peruana. *Revista Jurídica del Perú*, 55(63), pp. 33-55.

⁹ BLANCAS BUSTAMANTE, C. (2017). *Derecho Constitucional*. Lima: Fondo Editorial de la Pontificia Universidad Católica del Perú.

¹⁰ POMAREDA MUÑOZ, D. A. (2021). Los caminos de la nueva Constitución en el Perú: una propuesta democrática más allá de contextos particulares. *Revista LP Derecho*, (1), pp. 11-27.

innovaciones tecnológicas, y la jurisprudencia del Tribunal Constitucional (o su equivalente), cuya interpretación evolutiva, principios pro persona e interpretación conforme aseguran la coherencia del ordenamiento frente a cambios sociales, políticos y tecnológicos. En conjunto, estos mecanismos permiten que el diseño constitucional no se torne obsoleto y que el Estado mantenga su capacidad de gobernanza en contextos de rápida mutación.

Respecto a la reforma constitucional, esta busca adecuar el marco normativo a las condiciones y dinámicas de la realidad (García Toma, 2013)¹¹. Después de todo, la facultad de modificar las constituciones permite garantizar su perdurabilidad y estabilidad institucional (Rodríguez y Rodríguez y Melgarejo, 2019)¹². Por ello, la reforma constitucional resulta un elemento de vital importancia que permite la subsistencia de un Estado al adaptar su norma suprema a la realidad.

Por otro lado, el Tribunal Constitucional constituye el principal mecanismo de protección de la Constitución. Las interpretaciones que emite tienen carácter vinculante tanto para los ciudadanos como para todos los órganos que integran el Estado (Monroy Cabra, 2004)¹³. En ese sentido, dichas interpretaciones contribuyen al desarrollo de los contenidos de la Constitución. De tal modo que el tribunal ejerce el control sobre las normas y actos de los poderes constituidos, así como resolver los conflictos entre ellos. A su vez, resulta el órgano revisor encargado de determinar qué contenidos de la Constitución deben mantenerse o modificarse para adecuarse a una realidad sociopolítica en transformación, siempre bajo los límites de la propia Constitución (Carpizo, 2009)¹⁴.

¹¹ GARCÍA-TOMA, V. (2013). La reforma constitucional en el Perú: implicaciones y retos. *Athina*, (10), pp. 15-52. <https://doi.org/10.26439/athina2013.n010.1170>

¹² RODRÍGUEZ Y RODRÍGUEZ, S., & MELGAREJO, R. (2019). El cambio constitucional, sus vías y su abuso. *Revista Del Posgrado. En Derecho De La UNAM*, (7), pp. 22.

¹³ MONROY CABRA, M. G. (2004). Necesidad e importancia de los tribunales constitucionales en un Estado social de Derecho. En Konrad-Adenauer-Stiftung (Ed.). *Anuario de Derecho Constitucional Latinoamericano. Tomo I*, pp. 15-39.

¹⁴ CARPIZO, J. (2009). El tribunal constitucional y el control de la reforma constitucional. *Boletín Mexicano De Derecho Comparado*, 1(125).

Sintetizando lo desarrollado, la adaptación de la Constitución a los cambios sociales garantiza su vigencia y legitimidad en contextos históricos diversos, reafirmando su rol como reflejo dinámico de la identidad y valores de una comunidad. Para ello, tanto la reforma constitucional como la interpretación jurisdiccional constitucional actúan como mecanismos esenciales que permiten al Estado responder jurídicamente a las transformaciones sociales sin quebrar el orden constitucional.

A. Las nuevas tecnologías como un reto para el constitucionalismo

En el contexto actual, el constitucionalismo se enfrenta a múltiples desafíos, entre los cuales destaca la necesidad de adecuarse al impacto de las nuevas tecnologías. Esta preocupación no es reciente. Ya en 2008, Francisco Javier Díaz Revorio (2008)¹⁵ advertía que uno de los retos fundamentales de la Constitución consistía en su capacidad para adaptarse al desarrollo tecnológico. Si tal advertencia resultaba pertinente hace más de una década, su vigencia se acentúa aún más en la actualidad, marcada por el acelerado avance tecnológico y la aparición de nuevos fenómenos derivados de este proceso.

Actualmente, realizando una gran síntesis de los avances científicos, se puede considerar a las biotecnologías y a la inteligencia artificial como los productos más destacados. Al respecto, Giuseppe Franco Ferrari (2021)¹⁶ comentó que el avance de la biotecnología y la inteligencia artificial desdibujó la distinción clásica entre ciencia y tecnología. De esta forma, permitiendo intervenciones directas en la vida de las personas, pudiendo modificar aspectos biológicos de los humanos, como también maneja grandes cantidades de información en poco tiempo. Por lo que, resulta necesario asegurar la protección de los derechos humanos frente a ellas.

¹⁵ DÍAZ REVORIO, F. J. (2008). La Constitución ante los avances científicos y tecnológicos: breves reflexiones al hilo de los recientes desarrollos en materia genética y en tecnologías de la información y la comunicación. *Pensamiento Constitucional*, 13(13), pp. 203-226.

¹⁶ FERRARI, G. (2021). Los retos del constitucionalismo contemporáneo. *Revista AC Asuntos Constitucionales*, pp. 5-28.

A su vez, estos avances no deben restar relevancia de otros productos de las nuevas tecnologías, como las tecnologías de la información y comunicación, el *big data*, el Internet de las Cosas, la nanotecnología, la robótica y las plataformas digitales, que también transformaron, y siguen modificando, estructuras sociales y económicas e influyen en derechos como la privacidad, la libertad de expresión o el acceso a la información, entre otros. Por lo que, la Constitución debe evolucionar para abordar estos nuevos desafíos, garantizando que las nuevas tecnologías se desarrollen dentro de un marco que respete los derechos fundamentales. En este sentido, resulta imperativo que las reformas constitucionales y la jurisprudencia continúen jugando un papel clave, adaptando la norma suprema frente a los avances tecnológicos.

III. La potencial amenaza de las nuevas tecnologías a los derechos fundamentales

El informe de investigación *“Nuevas tecnologías y derechos humanos: impactos, desafíos y oportunidades en la era de la conectividad digital”*, señaló de forma acertada que, el desarrollo de las nuevas tecnologías y su uso en la vida de las personas avanza sin precedentes en comparación con años anteriores. Sin embargo, dichos avances tecnológicos no van de la mano con la creación y el desarrollo de los mecanismos de regulación que se necesitan, por lo que resulta preocupante advertir la falta de respuestas por parte de los Estados y las organizaciones ante los nuevos desafíos y amenazas que dichas tecnologías causan o pueden causar a la vida de las personas y, por ende, a sus derechos humanos (2023)¹⁷.

Lucena sostiene que el impacto actual y futuro de las nuevas tecnologías sobre los derechos humanos depende en gran medida de actores con intereses heterogéneos. Por ello, dichas agendas no siempre priorizan el respeto y la protección de tales derechos. En ese sentido, siguiendo a Ruíz y Pérez de Acá, enfatiza la necesidad de promover una responsabilidad tecnológica. Esto supone una actitud reflexiva, crítica y consciente frente a los problemas novedosos que la tecnología suscita en las diversas esferas de la vida. Asimismo, se trata de desafíos ante los cuales la sociedad y

17 MIRANDA, P., RUIZ, Y. & PULIDO, D. (2023). *Nuevas tecnologías y derechos humanos: Impactos, desafíos y oportunidades en la era de la conectividad digital*. Idehpucp & Fundación Fonrad Adenauer.

las disciplinas científicas, tecnológicas y humanísticas no deben permanecer indiferentes (2019)¹⁸.

La relación entre nuevas tecnologías y derechos fundamentales es compleja: no se trata simplemente de amenazas, sino de un campo de tensiones y oportunidades. En medio del entusiasmo por la innovación y la eficiencia, se ha abierto una creciente preocupación sobre el impacto que estas tecnologías pueden tener sobre el núcleo duro de los derechos fundamentales, tales como la privacidad, la libertad de expresión, la igualdad y el debido proceso.

Uno de los principales riesgos identificados se relaciona con la erosión del derecho a la privacidad. Así lo plasma P. Véliz, quien sostiene que, el sector tecnológico se ha beneficiado de una “invisibilidad” estructural, pues el entorno digital no se siente ni se pesa, de modo que la observación constante pasa desapercibida. En consecuencia, la sustracción de datos personales se percibe tarde, cuando revertir sus efectos es difícil (2020)¹⁹.

El uso extendido de sistemas de vigilancia, la recopilación masiva de datos personales por parte de Estados y corporaciones, y el escaso control que tienen los ciudadanos sobre la información que proporcionan, han configurado un escenario en el que la intimidad individual se ve constantemente amenazada. Así, tecnologías como el reconocimiento facial, el rastreo por GPS o los asistentes virtuales incorporan capacidades intrusivas que, en muchos casos, operan sin mecanismos claros de control democrático. Ello genera una tensión directa con el principio de autodeterminación informativa y evidencia la necesidad de establecer una regulación sólida que salvaguarde de manera efectiva la esfera privada.

A ello se suma el efecto que ciertos algoritmos pueden tener sobre la libertad de expresión y el acceso a la información. Las plataformas digitales, hoy fundamentales para el debate público, utilizan sistemas automatizados para moderar contenidos, priorizar noticias o recomendar

18 LUCENA CID, I. V. (2019). Las Nuevas Tecnologías y su impacto en los Derechos Humanos. Hacia un nuevo enfoque | New Technologies and their impact on Human Rights. Towards a new approach. *Cuadernos Electrónicos De Filosofía Del Derecho*, (40), pp. 128-146.

19 VÉLIZ, C. (10 de agosto de 2020). El desafío de la privacidad en la era tecnológica. *Ethic*.

publicaciones. Esta lógica algorítmica, muchas veces de carácter opaco, puede derivar en la censura de discursos legítimos, la propagación de desinformación o la creación de cámaras de eco que restringen la deliberación plural, lo que, en palabras textuales de Ordoñez, González-Sanabria y González “dificulta la formación de opiniones informadas y la diversidad de ideas” (2024, p. 6)²⁰. En contextos de autoritarismo, estas herramientas pueden, inclusive, ser empleadas como mecanismos de control y represión política.

Otro ámbito de preocupación es el impacto discriminatorio que pueden tener ciertas tecnologías, en cuanto reproducen y amplifican sesgos históricos, afectando especialmente a poblaciones vulnerables como mujeres, comunidades racializadas o personas con discapacidad (Iturmendi Rubia, 2023)²¹. Esta discriminación algorítmica, que opera en muchas ocasiones de forma inadvertida, refuerza desigualdades estructurales y contradice el principio de igualdad ante la ley. Asimismo, la creciente automatización de decisiones en el ámbito público y privado plantea desafíos relevantes al debido proceso, como en el caso explicado de Colombia. La delegación de decisiones a sistemas inteligentes puede conducir a resultados injustos si no se garantizan el derecho a ser oído, la revisión humana y la motivación de las decisiones. La justicia, entendida como un proceso dialógico y garantista, no puede reducirse a la ejecución de códigos opacos sin *accountability*.

No obstante, sería un error concebir a las nuevas tecnologías únicamente como amenazas. En muchos casos, pueden convertirse en herramientas valiosas para la realización de los derechos fundamentales. En zonas rurales o aisladas, por ejemplo, las plataformas digitales han permitido el acceso a servicios básicos. Verbigracia, salud, educación y justicia. En ese sentido, es válido afirmar que la conectividad, bien gestionada, puede cerrar brechas de exclusión y favorecer procesos de inclusión social. Asimismo, tecnologías como *blockchain* han abierto caminos interesantes en materia de transparencia gubernamental y lucha contra la corrupción, mientras que la inteligencia artificial, tal y como ha sido analizado

²⁰ GONZÁLEZ ARENCIBIA, M., ORDOÑEZ ERAZO, H., & González-Sanabria, J.-S. (2024). ¿Tienen Derechos los Algoritmos? *Praxis & Saber*, 15(43), pp. 1-21.

²¹ ITURMENDI RUBIA, J. M. (2023). Algorithmic discrimination and its impact on human dignity and human rights. Special reference to immigrants. *Deusto Journal of Human Rights*, (12), pp. 257-284.

acápites anteriores, puede ser una aliada en la eficiencia judicial.

Además, la participación ciudadana encontró nuevas formas de expresión gracias a las tecnologías digitales. Movimientos sociales, denuncias de violencia institucional y procesos de organización colectiva ganaron visibilidad y potencia gracias a las redes, ampliando los márgenes del espacio público y democratizando la deliberación (Del Prado, Robaina y Minteguiaga, 2023)²². Desde esta perspectiva, las tecnologías no son neutras. En realidad, su potencial emancipador o regresivo depende de su diseño, implementación y regulación.

El desafío central contemporáneo consiste en diseñar una gobernanza tecnológica centrada en los derechos humanos; ello supone asumir que el desarrollo técnico debe someterse a principios como legalidad, necesidad, proporcionalidad, transparencia y rendición de cuentas. En consecuencia, los Estados han de establecer marcos normativos que protejan a las personas frente a usos indebidos, promuevan la equidad en el acceso a la digitalización y exijan responsabilidad a quienes conciben e implementan estas herramientas. Asimismo, resulta imprescindible la participación activa de la sociedad civil, la academia y el sector tecnológico para construir, de manera crítica y democrática, un futuro digital compatible con la dignidad y las libertades fundamentales.

IV. Análisis comparativo de las respuestas constitucionales frente al problema bajo análisis

En contextos donde las Constituciones no incorporaron de forma expresa disposiciones sobre las nuevas tecnologías, la jurisprudencia constitucional y la normativa de rango legal asumieron un papel decisivo en la protección de los derechos fundamentales frente a los desafíos del entorno digital. Este apartado examina cómo ciertos países latinoamericanos, Ecuador, México, Colombia, Bolivia y Perú desarrollaron respuestas judiciales como normativas frente a fenómenos como la inteligencia artificial, las tecnologías de la información y la afectación a la privacidad.

²² DEL PRADO, L., ROBAINA, N., & MINTEGUIAGA, M. (2023). Discusiones y conclusiones de la sección. En L. Del Prado & M. Suárez (Eds.), *Las tecnologías digitales y los procesos de participación ciudadana: ¿Una diada para la transformación social?* (pp. 66-68). CLACSO.

i. Ecuador

La Constitución ecuatoriana de 2008 reconoce indirectamente el acceso a las nuevas tecnologías como derecho (artículos 16°, 17° y 385°), garantiza la libertad de expresión en entornos digitales y promueve la ciencia y la tecnología (2008). No obstante, el análisis de Sánchez Sánchez (2023)²³ evidencia la necesidad de actualizar permanentemente el marco que regula la libertad de expresión y el acceso y uso de las TIC para asegurar su correcta aplicación, dada su centralidad para otras libertades en el ámbito digital. Además, el texto constitucional no contempla expresamente los neuroderechos, aunque se advierte un interés estatal creciente que podría habilitar futuros debates y eventuales reformas

No obstante, y pese a que su Constitución, no presenta un apartado directo relacionado con las nuevas tecnologías como lo es la bioética, inteligencia artificial o similares, si existe un desarrollo jurisprudencial al respecto por parte de su órgano encargado de la interpretación de la Constitución. En ese sentido, partimos con CASO No. 456-20-JP, en el cual la Corte Constitucional de Ecuador abordó un caso en el que una estudiante fue sancionada con la suspensión y el decomiso de su teléfono móvil por reenviar imágenes íntimas de una compañera (acto vinculado al fenómeno del *sexting*).

A su vez, la Corte Constitucional examinó los procedimientos disciplinarios aplicados en el contexto educativo desde la perspectiva de la justicia restaurativa, así como del derecho al debido proceso y sus garantías. Como resultado del análisis, el tribunal concluyó que en dicho caso específico se produjo una vulneración de estos derechos fundamentales. Del caso mencionado, lo que resulta de principal interés es el fundamento catorce, el cual señala que las TIC facilitan el desarrollo de nuevas formas de autonomía e independencia en las personas, al tiempo que posibilitan la creación de entornos digitales que fomentan la interacción y socialización entre los adolescentes (Corte Constitucional de Ecuador, 2021)²⁴.

²³ SÁNCHEZ SÁNCHEZ, W. Y. (2023). *Tecnologías de la información y comunicación, incidencia en el derecho a la libertad de expresión, Ecuador* [Tesis de pregrado, Universidad Regional Autónoma de los Andes]. Repositorio UNIÁNDES. <https://dspace.uniandes.edu.ec/bitstream/123456789/16833/1/UA-DER-EAC-011-2023.pdf>

²⁴ Corte Constitucional del Ecuador. (2021). *Sentencia No. 456-20-JP/21: Caso No. 456-20-JP*.

De tal modo que la Corte reconoce el impacto transformador de las nuevas tecnologías en la vida cotidiana y en el desarrollo de capacidades, particularmente en adolescentes, destacando tanto su potencial para fortalecer derechos fundamentales como sus riesgos. Aunque la Constitución ecuatoriana no prevé un régimen específico para fenómenos como la IA o la bioética, la jurisprudencia constitucional viene reinterpretando los derechos a la luz de los desafíos y oportunidades que introduce la digitalización.

ii. México

En el caso de México, se observa un escenario similar al ecuatoriano, en la medida en que su Constitución Política carece de una referencia explícita a las nuevas tecnologías. No obstante, incorpora disposiciones como el artículo 3º que reconocen el derecho de toda persona a disfrutar de los beneficios del desarrollo científico y de la innovación tecnológica. Por su parte, el artículo 6º dispone que el Estado debe asegurar el derecho de acceso a las tecnologías de la información y la comunicación, así como a los servicios de radiodifusión y telecomunicaciones, incluidos la banda ancha y el Internet (1917)²⁵.

A su vez, a través de una sólida línea jurisprudencial desarrollada por la Suprema Corte de Justicia de la Nación, órgano que, por analogía funcional, asume las competencias propias de un tribunal constitucional, se han abordado temas vinculados al desarrollo tecnológico. Un ejemplo clave de esta jurisprudencia es el pronunciamiento relacionado con el artículo 185 Bis C del Código Penal de Sinaloa, el cual tipifica el uso de la inteligencia artificial para manipular contenido íntimo de carácter sexual sin el consentimiento expreso de la persona afectada. En este caso, la Suprema Corte validó la constitucionalidad de la definición de IA contenida en dicha disposición, argumentando que el uso de esta tecnología para vulnerar la privacidad y la dignidad de las personas representa una violación grave de los derechos humanos, en particular de la privacidad, el consentimiento y la integridad personal. De esta manera, la Corte reafirmó su compromiso con la protección de los

²⁵ México. (1917). *Constitución Política de los Estados Unidos Mexicanos*. Diario Oficial de la Federación.

derechos fundamentales en un contexto digital (Suprema Corte de Justicia de la Nación, 2025)²⁶.

Este pronunciamiento refleja cómo, a pesar de la falta de un marco explícito en la Constitución sobre las nuevas tecnologías, el sistema judicial puede adaptar la interpretación de la norma constitucional a los retos emergentes. Utilizando el principio de interpretación conforme, la Corte aseguró que las leyes y disposiciones locales deben adecuarse a los estándares constitucionales, protegiendo los derechos fundamentales frente a los avances tecnológicos. Este enfoque dinámico resalta la necesidad de que las legislaciones locales, como la de Sinaloa, se mantengan actualizadas ante las nuevas formas de violencia digital.

iii. Colombia

Para el caso de Colombia, su Constitución no incorpora una cláusula expresa sobre nuevas tecnologías. El término tecnología aparece principalmente vinculado al fomento científico-educativo y productivo: la educación orientada al acceso a la ciencia y la técnica y al mejoramiento tecnológico (artículo 67°), la promoción de la enseñanza científica y técnica (artículo 70°), los incentivos estatales a la ciencia y la tecnología (artículo 71°) y la investigación y transferencia de tecnología en el sector agropecuario (artículo 65°). De forma complementaria, se regulan insumos tecnológicos, como el espectro electromagnético y las telecomunicaciones, y se tutelan ámbitos correlativos, hábeas data y comunicaciones privadas (1991)²⁷, sin emplear de manera explícita la expresión nuevas tecnologías o relacionados.

Empero, es de destacar cierta jurisprudencia, por ejemplo, la Sentencia T-323 de 2024 de la Corte Constitucional de Colombia²⁸ representa un hito jurisprudencial al abordar, por primera vez con profundidad, el uso de IA por parte de un juez para fundamentar su decisión en un proceso de tutela. Esta sentencia no solo ofrece lineamientos sobre el uso responsable de la IA en el ámbito judicial, sino que también sitúa a Colombia entre los

²⁶ Suprema Corte de Justicia de la Nación. (2025, 20 de febrero). *Valida la Corte definición de inteligencia artificial establecida en el Código Penal del Estado de Sinaloa* [Comunicado de prensa No. 055/2025]. <https://www.internet2.scjn.gob.mx/red2/comunicados/comunicado.asp?id=8175>.

²⁷ Colombia. (1991). *Constitución Política de Colombia*.

²⁸ Sentencia T-323 de 2024. (2024). Corte Constitucional de Colombia.

países que reconocen y problematizan constitucionalmente el impacto de las nuevas tecnologías.

La controversia que dio origen a esta sentencia surgió cuando un juez de segunda instancia, al resolver una acción de tutela sobre el derecho a la salud de un niño diagnosticado con Trastorno del Espectro Autista, recurrió al uso de ChatGPT para complementar su razonamiento. Este hecho generó inquietudes respecto a si se había vulnerado el derecho fundamental al debido proceso, al poner en duda si la decisión fue verdaderamente adoptada por un juez de la República o si, por el contrario, se delegó indebidamente a un sistema automatizado.

A partir de ello, la Corte Constitucional evaluó una doble dimensión: por un lado, el fondo del caso, la garantía del derecho a la salud integral del menor y la eliminación de barreras administrativas como copagos y falta de transporte; y por otro, la legitimidad constitucional del uso de IA en la actividad jurisdiccional, concluyendo que, en el caso concreto, sí se garantizó el derecho a la salud del menor, pues se ordenó la eliminación de barreras administrativas como copagos y la falta de transporte, reafirmando con ello su especial protección constitucional. Al mismo tiempo, coligió que el uso de inteligencia artificial por parte del juez no vulneró el debido proceso, pues no sustituyó la función judicial ni comprometió la motivación autónoma de las decisiones.

Al respecto, la decisión urge regular la IA en la justicia con lineamientos claros, anclando su legitimidad en transparencia, responsabilidad y respeto al juez natural. Exige sistemas explicables y auditables, trazabilidad y rendición de cuentas, y prohíbe delegar decisiones jurisdiccionales a procesos plenamente automatizados para resguardar el debido proceso. Reconoce el potencial y los riesgos de la tecnología y demanda vigilancia jurídica continua con evaluaciones de impacto y controles ex ante y ex post, proponiendo una incorporación prudente que preserve los derechos fundamentales.

iv. Bolivia

La Constitución boliviana de 2009, en su artículo 103, impone al Estado el deber de impulsar y financiar la ciencia y la tecnología mediante un sistema estatal y políticas para incorporar las TIC. Además, dispone un enfoque colaborativo e inclusivo, Estado, universidades, empresas públicas y privadas y naciones y pueblos indígena originario campesinos,

para investigar, innovar, difundir, aplicar y transferir conocimiento, con el fin de fortalecer la base productiva y el desarrollo integral de la sociedad, en línea con modelos que priorizan el beneficio social de la tecnología (Estado Plurinacional de Bolivia, 2009)²⁹.

Bolivia impulsa una modernización institucional para integrar TIC en los ámbitos judicial y administrativo, buscando agilizar trámites, transparentar actuaciones y ampliar el acceso a justicia y servicios públicos. Aunque existe un marco normativo favorable a la digitalización, su efectividad exige combinar inversión en infraestructura con formación continua. Como advierte Fernando Núñez (2021)³⁰, los operadores, en especial los administradores de justicia, necesitan capacitación sostenida para usar adecuadamente las aplicaciones y operativizar los sistemas electrónicos. En suma, la modernización solo será exitosa si converge con el fortalecimiento técnico y la adaptación organizacional.

Sin embargo, a pesar de estos esfuerzos de modernización, persisten limitaciones estructurales en el marco constitucional vigente. De acuerdo con Romero (2025), “La Constitución Política del Estado de Bolivia (2009) presenta insuficiencias significativas para la protección efectiva de los derechos digitales en el contexto tecnológico actual, caracterizado por el desarrollo acelerado de las TICs y la inteligencia artificial” (p. 2109)³¹. Este desfase normativo se debe en gran parte a que el texto constitucional fue concebido en un momento histórico previo a la consolidación de fenómenos como la expansión de las redes sociales, la economía de datos y la automatización de decisiones mediante inteligencia artificial.

El mismo autor detalla estas debilidades al enumerar las limitaciones del marco constitucional actual:

- Déficit de conceptualización: ausencia de conceptos rectores tales como datos personales, identidad digital, neutralidad de la red y decisiones automatizadas.

²⁹ Estado Plurinacional de Bolivia. (2009). *Constitución Política del Estado Plurinacional de Bolivia*.

³⁰ Núñez Jiménez, F. (2021). El uso de la tecnología en la administración de justicia en Bolivia. *Perspectivas*, (5).

³¹ Romero Cárdenas, F. (2025). La Brecha entre la Constitución y la Realidad: Los Derechos Digitales Emergentes en Bolivia frente a la Inteligencia Artificial (2019-2024). *Revista Veritas De Difusão Científica*, 6(2), pp. 2084–2112.

- Déficit de herramientas institucionales específicas orientadas a la defensa de los derechos en el ecosistema digital.
- Déficit de armonización con el marco internacional: ausencia de adecuación a principios en evolución recogidos por el *hard y soft law* en derechos digitales (2025).

Esta combinación de avances tecnológicos institucionales y deficiencias constitucionales genera un escenario de protección desigual; mientras que, en el plano administrativo y judicial se promueve el uso de herramientas digitales, en el plano normativo supremo no existen garantías claras que respalden de forma integral los derechos fundamentales frente a los riesgos de la era digital. En este sentido, resalta la necesidad de una reforma constitucional que actualice su lenguaje, incorpore conceptos contemporáneos y adopte compromisos con estándares internacionales, de modo que la innovación tecnológica se traduzca efectivamente en la protección y promoción de los derechos de la ciudadanía.

v. Perú

La Constitución Política de 1993 no contiene una referencia expresa a los derechos digitales ni a la regulación de las nuevas tecnologías, lo que evidencia un marco normativo primario carente de disposiciones específicas frente a los desafíos derivados de la sociedad de la información. No obstante, diversos preceptos constitucionales, como el derecho a la intimidad personal y familiar (artículo 2°, inciso 7), el derecho al secreto y a la inviolabilidad de las comunicaciones (artículo 2°, inciso 10) y la libertad de información, opinión, expresión y difusión del pensamiento (artículo 2°, inciso 4), proporcionan una base interpretativa para extender su protección al entorno digital.

En el plano legislativo, se dictaron normas que, aunque no forman parte del texto constitucional, atienden aspectos particulares de la realidad tecnológica. Entre ellas, destacan la Ley 29733, Ley de Protección de Datos Personales, y su reglamento. De igual modo, la Ley 30096, Ley de Delitos Informáticos, tiene por objeto prevenir y sancionar aquellas conductas ilícitas que, mediante el uso de tecnologías de la información o de la comunicación, afecten sistemas, datos informáticos u otros bienes jurídicos de relevancia penal, con el propósito de fortalecer la eficacia en la lucha contra la ciberdelincuencia.

A su vez, se cuenta con la Ley 31814, Ley que promueve el uso de la inteligencia artificial en favor del desarrollo económico y social del país. Por lo que, se observa que, en el apartado legislativo, existen diversos esfuerzos por reconocer la importancia de incorporar marcos normativos que orienten el uso responsable y ético de las tecnologías emergentes, fomenten la innovación y, al mismo tiempo, salvaguarden los derechos fundamentales de las personas, procurando un equilibrio entre el impulso al desarrollo tecnológico y la protección de la dignidad humana.

Sin embargo, la ausencia de una cláusula constitucional explícita sobre derechos digitales genera incertidumbre normativa y limita la capacidad del ordenamiento para responder de forma integral a fenómenos emergentes como la inteligencia artificial, el *big data*, la vigilancia masiva o la brecha digital. En tal sentido, si bien el ordenamiento jurídico peruano avanzó en la aprobación de normas sectoriales orientadas a regular aspectos específicos del ecosistema digital, la falta de un reconocimiento constitucional autónomo impide consolidar un marco de protección coherente y jerárquicamente robusto.

vi. Chile

El caso chileno destaca de los anteriores países desarrollados en que su Constitución cuenta con una mención expresa de la finalidad de las nuevas tecnologías y realiza énfasis en uno de sus campos en particular. Señalado ello, la Constitución chilena de 1980 muestra en el último párrafo del inciso 1 del artículo 19 lo siguiente:

El desarrollo científico y tecnológico estará al servicio de las personas y se llevará a cabo con respeto a la vida y a la integridad física y psíquica. La ley regulará los requisitos, condiciones y restricciones para su utilización en las personas, debiendo resguardar especialmente la actividad cerebral, así como la información proveniente de ella (Chile, 1980)³².

En relación con lo mencionado, esta disposición fue incorporada mediante la Ley 21.383, Ley que Modifica la Carta Fundamental para Establecer el Desarrollo Científico y Tecnológico al Servicio de las Personas, promulgada en 2021. A partir de esta norma, se desprende que el Poder Legislativo asume la responsabilidad de regular los aspectos

³² Chile. (1980). *Constitución Política de la República de Chile* (Actualizada hasta el 19 de enero de 2024). Biblioteca del Congreso Nacional de Chile.

esenciales del uso de las nuevas tecnologías en las personas. Asimismo, la reforma destaca la importancia de resguardar los neuroderechos, entendidos como una rama emergente del derecho encargada de normar los avances tecnológicos que afectan directa o indirectamente al cerebro humano (Gutiérrez Otiniano y Chocano Ravina, 2024)³³.

Entre los casos analizados, la Constitución de Chile es la que mejor se adecúa a los cambios tecnológicos, al incorporar una reforma expresa que no solo reconoce el desarrollo científico-tecnológico al servicio de la persona, sino que también constitucionaliza la protección de los neuroderechos. Con ello, Chile se posiciona como referente regional en gobernanza tecnológica, pues no se limita a promover la innovación, sino que establece límites y principios éticos claros para su aplicación, en particular respecto de la actividad cerebral y la información neuronal.

A continuación, se presenta un cuadro resumen que sintetiza las principales fuentes y enfoques analizados en cada uno de los países objeto de estudio, permitiendo visualizar de forma comparativa las diferencias y similitudes en sus respuestas jurídicas frente a los retos que plantean las nuevas tecnologías.

³³ GUTIÉRREZ, J., & CHOCANO, E. (2024). ¿Debemos incluir en la constitución política del Perú un apartado sobre las nuevas tecnologías? Una respuesta desde una constitución cultural. *Acta Jurídica Peruana*, 7(2), pp. 39-50.

País	Fuente analizada	Tipo de respuesta jurídica	Ejemplo relevante	Periodo
Chile	Constitución (artículo sobre neuroderechos)	Reforma constitucional	Incorporación de neuroderechos a la Constitución	1980 -actualidad
México	Jurisprudencia constitucional	Interpretación judicial	Sentencias SCJN sobre privacidad y datos personales	1917 -actualidad
Colombia	Jurisprudencia constitucional	Interpretación judicial	Corte Constitucional: casos sobre habeas data y plataformas digitales	1991 -actualidad
Ecuador	Jurisprudencia constitucional	Interpretación judicial	Protección de derechos frente a vigilancia digital	2018 -actualidad
Bolivia	Constitución (2009) y marco legal sobre TIC en la administración pública	Modernización administrativa con limitaciones constitucionales	Incorporación de TIC en el sistema judicial y administrativo, con déficit de protección constitucional en derechos digitales	2009 -actualidad
Perú	Constitución (1993) y legislación sectorial	Normas legislativas complementarias	Ley de Protección de Datos Personales, Ley de Delitos Informáticos, Ley de IA; sin reconocimiento constitucional explícito de derechos digitales	1993 -actualidad

Elaboración propia

V. Discusión: crítica sobre la positivación constitucional de reglas sobre nuevas tecnologías y sobre las respuestas estatales descritas

Díaz y Castro (2021)³⁴ sostienen que el siglo XXI se distingue por la inserción intensa y transversal de las tecnologías de la información y comunicación en la vida cotidiana; desde que despertamos hasta el final del día, nuestras actividades se hallan mediadas por ellas, siendo el teléfono móvil su manifestación más visible. Por ello, resulta pertinente cuestionarse si es necesario replantear el paradigma de protección de los derechos fundamentales, considerando la importancia de construir un enfoque común frente a estas tecnologías. Esto se debe a que los desafíos éticos y jurídicos que surgen tanto en su regulación, en las etapas de investigación, diseño, implementación y uso, como en la garantía constante del pleno respeto a los derechos fundamentales, presentan similitudes sustanciales en distintos contextos (Benlloch & Sarrión, 2022).³⁵.

En la actualidad, varios Estados evalúan constitucionalizar los derechos digitales, el acceso a la tecnología y la protección de datos, planteando la pregunta sobre la oportunidad y pertinencia de esa positivización. Los autores ofrecen una reflexión crítica al respecto, profundizando en argumentos previos. Desde la teoría constitucional, la Carta Magna estructura el poder, garantiza derechos y expresa valores fundamentales; por ello, incorporar explícitamente las nuevas tecnologías implica reconocer su papel estructurante en la vida contemporánea y asegurar que principios democráticos, como la dignidad y la justicia, se mantengan protegidos en un entorno crecientemente digitalizado, alineando el diseño institucional con la realidad tecnológica.

No obstante, también supone un desafío de técnica jurídica: ¿cómo constitucionalizarlo que está en constante mutación? Positivizar las nuevas tecnologías no es simplemente nombrarlas en el texto constitucional,

³⁴ DÍAZ COLCHADO, J. C., & CASTRO AREQUIPEÑO, A. (2021). Los Derechos Fundamentales y las nuevas tecnologías de la Información y Comunicación: una aproximación. *THEMIS Revista De Derecho*, (79), pp. 15-35.

³⁵ BENLLOCH DOMENECH, C., & SARRIÓN ESTEVE, J. (2022). Los derechos fundamentales ante las aporías de la era digital. *Cuestiones Constitucionales. Revista Mexicana De Derecho Constitucional*, 1(46), pp. 3-28.

sino otorgarles un estatus normativo que permita estructurar la acción del Estado, guiar el desarrollo legislativo y garantizar derechos fundamentales en el entorno digital. Uno de los principales argumentos a favor de la positivización radica en el reconocimiento de nuevos derechos fundamentales. El acceso a internet, la protección de datos personales, la neutralidad de la red, el derecho a la desconexión digital o incluso la autodeterminación informativa son expresiones de una ciudadanía que ya no se ejerce exclusivamente en el espacio físico, sino también, y cada vez más, en el digital. En ese contexto, constitucionalizar estos derechos puede fortalecer su exigibilidad, blindarlos frente a retrocesos legislativos y garantizar que el desarrollo tecnológico se oriente hacia la inclusión, la equidad y la dignidad humana.

Este argumento fue planteado con contundencia en el artículo “*Four Ethical Priorities for Neurotechnologies and AI*”, elaborado por 25 científicos en la Universidad de Columbia (Yuste *et al.* 2017)³⁶. En dicho texto, los autores recomiendan la incorporación de cláusulas específicas que protejan los neuroderechos en tratados internacionales, incluyendo instrumentos como la Declaración Universal de Derechos Humanos de 1948. Sin embargo, conscientes de las limitaciones jurídicas de estos mecanismos, específicamente por su carácter no vinculante, proponen la creación de una convención internacional que defina de forma clara las conductas prohibidas en el uso de la neurotecnología y la inteligencia artificial.

Otro aspecto relevante es que la incorporación constitucional de principios vinculados a la tecnología puede reafirmar el rol activo del Estado como garante del interés público en el entorno digital.

Sin embargo, la positivización constitucional también presenta importantes riesgos. El más evidente es el peligro de obsolescencia normativa. La velocidad con la que evoluciona la tecnología puede dejar rápidamente desactualizadas disposiciones que, al momento de su redacción, responden a realidades técnicas o sociales muy distintas. Ello puede generar normas inoperantes o demasiado genéricas, que pierden capacidad reguladora o se limitan a ser declaraciones simbólicas.

³⁶ YUSTE, R., et al. (2017). Four ethical priorities for neurotechnologies and AI. *Nature*, 551(7679), pp. 159-163.

Asimismo, la rigidez propia de los textos constitucionales, dada la dificultad de su reforma, puede ser contraproducente frente a un entorno que exige adaptabilidad y respuestas ágiles. En este sentido, existe el riesgo de que al constitucionalizar cuestiones tecnológicas de manera excesivamente técnica o específica, se entorpezca la evolución del marco jurídico o se introduzcan elementos que queden rápidamente desfasados.

Frente a estos dilemas, una propuesta intermedia y más prudente consiste en introducir en la Constitución principios programáticos que reconozcan la centralidad de las tecnologías digitales, sin caer en el tecnodeterminismo normativo. En lugar de describir tecnologías concretas, se pueden establecer obligaciones estatales generales, como garantizar un entorno digital respetuoso de los derechos humanos, promover el acceso equitativo a la información y proteger la integridad y la privacidad de las personas frente a los riesgos del uso de tecnologías automatizadas. Este enfoque permite combinar estabilidad normativa con flexibilidad interpretativa, facilitando que los jueces, legisladores y órganos técnicos actualicen su sentido conforme al desarrollo de los contextos.

Así, este apartado se convierte en una oportunidad para acotar que la positivización constitucional de las nuevas tecnologías es, en esencia, una oportunidad para fortalecer la protección de los derechos fundamentales y consolidar un modelo de desarrollo digital centrado en el ser humano. Su conveniencia depende del modo en que se formule. La clave está en no caer en la fascinación tecnocrática ni en la inercia jurídica, sino en construir un marco constitucional que dialogue con la innovación, sin perder su vocación de justicia, libertad e inclusión.

VI. Conclusiones

El análisis comparado de Colombia, México, Ecuador, Bolivia, Perú y Chile revela que, aunque todos comparten la intención de garantizar derechos fundamentales frente a las transformaciones sociales y tecnológicas, persisten diferencias sustanciales en el modo y la intensidad con que sus marcos constitucionales y judiciales han respondido a los desafíos de la era digital.

En Colombia y México, la jurisprudencia desempeña un papel decisivo al adaptar la interpretación de los derechos a entornos tecnológicos y

cubrir vacíos normativos; Bolivia impulsa la modernización tecnológica de su sistema judicial, aunque enfrenta retos de capacitación, adecuación normativa y acceso equitativo. En Ecuador se establecieron principios orientados a la protección de derechos digitales cuya eficacia exige reformas y actualizaciones constantes. En Perú, la tutela frente al uso de tecnologías se articula principalmente mediante legislación ordinaria, con limitada consagración expresa en el texto constitucional, lo que plantea el desafío de integrar dicha protección a un nivel superior para reforzar coherencia y seguridad jurídica.

Un caso distinto es Chile, quien sobresale frente a los demás países analizados por contar con una disposición constitucional explícita sobre la finalidad de las nuevas tecnologías. Esta formulación no solo es única en la región, sino que marca un precedente sumamente relevante al incorporar de forma directa en el texto constitucional la protección de aspectos tan sensibles como la neuroinformación, anticipando debates éticos y jurídicos de alcance global.

En conjunto, la experiencia de estos Estados evidencia que la adaptación al contexto digital requiere un doble esfuerzo, esto es, tanto reformas constitucionales y legales que reconozcan derechos y principios específicos para el entorno tecnológico, como sistemas judiciales dotados de herramientas y capacitación para garantizar su aplicación. A la vez, es menester resaltar que la incorporación de tecnología en los sistemas judiciales debe entenderse como un medio para mejorar la transparencia, la celeridad y el acceso a la justicia, buscando asegurar la protección de datos, las garantías procesales y la igualdad ante la ley.

Prevención delictiva basada en inteligencia artificial: Reflexiones en torno al derecho a la igualdad

Camila Parodi Ccoriñaupa*

Resumen.- Los sistemas inteligentes para prevenir delitos en el ciberespacio, especialmente agresiones sexuales contra menores enfrentan desafíos entre la eficacia preventiva y la igualdad. La opacidad algorítmica y la ausencia de regulación eficaz facilitan arbitrariedades. Por ello, se debe contar con un marco normativo que armonice adecuadamente la finalidad preventiva y exija la transparencia en su implementación.

Palabras clave.- Igualdad – Ciberespacio – Algoritmos - Discriminación.

Abstract.- Intelligent systems to prevent crimes in cyberspace, particularly sexual offenses against minors, face challenges in balancing preventive effectiveness and equality. Algorithmic opacity and the absence of effective regulation enable arbitrariness. Therefore, a regulatory framework is needed to adequately harmonize the preventive purpose and require transparency in its implementation.

Keywords.- Equality – Cyberspace – Algorithms - Discrimination.

* Estudiante de cuarto año de la carrera de derecho, asistente de cátedra en Derecho Penal y miembro principal del Taller de Dogmática Penal en la Universidad Nacional Mayor de San Marcos.

Nota: En memoria de Joseph Maykol Rolando Rodríguez Chavarry, cuya amistad y cariño seguirán vivos en cada recuerdo.

I. Introducción

El nuevo paradigma de la sociedad quebranta los elementos del tiempo, lugar y espacio conocidos en la narrativa de la humanidad. Este panorama ha derivado del fortalecimiento de las tecnologías de la información y comunicación (TIC), evidenciándose una interdependencia entre la evolución de la sociedad y el desarrollo del conocimiento científico. En este marco, es innegable que estas herramientas ostentan un valor social fundamental en el contexto de la globalización, donde la interacción humana trasciende fronteras y se convierte en un proceso de integración económica, política y cultural. Sin embargo, con el incesante desarrollo, los riesgos ocupan mayor preocupación que las numerosas ventajas de la tecnología.

La diversificación de la criminalidad trae consigo nuevas conductas delictivas que se encuadran dentro del ciberespacio, donde su potencialidad práctica no encuentra límites claros. En este contexto, la delincuencia supera lo conocido por el derecho tradicional y, en consecuencia, exhorta repensar las instituciones jurídicas convencionales.

Todo ello resulta de gran importancia en el mundo de los menores de edad, los sujetos que se encuentran profundamente vinculados con este nuevo escenario. Los nativos digitales desarrollan su personalidad a través de la red, en esta se comunican, informan y entretienen con mayor rapidez que la habitual realidad fáctica. Debido a dicha familiaridad tecnológica, este grupo demográfico se encuentra más propenso a ser víctima de aquellos agresores sexuales que esconden su rostro tras la pantalla, donde gozan de inmediatez y sutileza para perjudicar el adecuado desarrollo de la sexualidad de los menores de edad.

Sumado a ello, una encuesta realizada en el 2023 por el Instituto de Estudios Peruanos (IEP) reveló que más de 500.000 menores de edad recibieron solicitudes para que envíen fotos de su cuerpo y más de 570.000 niñas, niños y adolescentes conocieron a su agresor. Aunado a esto, el Perú es el segundo país en la región con más niños que han entablado conversaciones con extraños en línea. En particular, de acuerdo con el Primer Encuentro de *Grooming* Latam se indicó que a nivel regional el 41% de los casos implica amigos virtuales que solicitaron una relación más allá de una amistad, mientras que en el 21% de los casos, les solicitaron imágenes o videos de contenido íntimo.

Al comparar estas evidencias no cabe duda de que, la situación crítica en la que se encuentra el Perú exhorta adoptar medidas urgentes para contrarrestar estas cifras. Ante ello, surgen diversos problemas respecto a la forma de evitar o prevenir estos actos que afectan la indemnidad sexual, honor y otros derechos fundamentales. Sirva de ilustración los métodos fundados en la concientización social, en la cual se exponen los peligros que se expresan en el entorno digital y se educa a los padres de familia para tener conocimiento sobre cómo actuar ante estas situaciones.

No obstante, en los últimos años surgió la propuesta de combatir estas prácticas mediante la implementación de sistemas de inteligencia artificial. Para ello, se plantea hacer uso de la misma tecnología para identificar la dinámica seguida por los perfiles del espacio cibernético y perseguir a los potenciales agresores sexuales.

A pesar de lo beneficioso que puede resultar, muchos de estos programas –que en diversas partes del mundo están siendo utilizados como policía predictiva– trabajan en base a algoritmos, los cuales automatizan el proceso preventivo y ejecutan una relación de datos que permite un direccionamiento especial de las fuerzas de seguridad. En atención a ello, estos sistemas pueden orientarse por criterios raciales, socioeconómicos y de otra índole que podrían involucrar una diferenciación injustificada, pues se vincula con categorías sospechosas que transgreden el derecho a la igualdad y no discriminación.

Esta investigación pretende exponer la peligrosidad de las agresiones sexuales en el entorno digital y analizar si el uso de sistemas automatizados para la prevención de estas prácticas delictivas es legítimo en la actualidad, todo esto a la luz del derecho a la igualdad.

II. Desarrollo del estado de la cuestión y conceptos fundamentales

i. El ciberespacio como nueva realidad

La Real Academia Española define que el “ciberespacio” es producto de la conjunción de los medios informáticos, en otros términos, se trata de un espacio inmaterial caracterizado por el uso de las redes sociales, los archivos digitales y otras herramientas que permiten la transmisión de información en la red. En ese sentido, se trata de un nuevo ámbito social (una nueva realidad) que facilita la conectividad y el flujo comunicativo,

fortaleciendo la interacción en sociedad de la mano con la inteligencia artificial, el *big data* y elementos propios de esta dimensión¹.

Las descripciones anteriores manifiestan que la existencia del ser humano ya no se encuentra limitada a la materialidad tradicional, sino que se han abierto innumerables posibilidades para la transmisión de ideas, datos y cualquier tipo de información a nivel universal. No es para menos que en el 2019, la Estrategia Nacional de Ciberseguridad (en adelante, ENC) del Reino de España catalogó al ciberespacio como un “espacio común global caracterizados por su apertura funcional y su dinamismo”.

Sin embargo, los infinitos beneficios que puede ofrecer esta versatilidad digital contraponen la aparición de nuevos riesgos en la convivencia social; de modo que, la regulación normativa se encuentra notoriamente desafiada. Al respecto, la ENC distingue que el ciberespacio se asemeja a un “campo de batalla”, esto es, un escenario de confrontación donde la información y la privacidad son activos de incalculable valor, resultando en un contexto complicado para la protección de los derechos fundamentales.

Entre dichos retos se encuentra el desarrollo de nuevas formas de criminalidad, más sutiles y difícilmente localizables. La denominada cibercriminalidad se constituye como un fenómeno que transforma la comprensión habitual de la actividad delictiva y de los mecanismos para su prevención². Como muestra, se evidencia una especial preocupación por los delitos cibernéticos que afectan a niños, niñas y adolescentes, entre los cuales se encuentra el *child grooming* o acoso cibernético³.

¹ TÁVORA, M. (2022). *Vigilancia e investigación policial en el ciberespacio: aspectos procesales del ciberpatrullaje* [Tesis doctoral, Universidad de Sevilla]. Repositorio institucional de la Universidad de Sevilla. <https://dialnet.unirioja.es/servlet/tesis?codigo=309409>

² ROBLES, M. (2025). El ciberespacio y la ciberseguridad: Consideraciones sobre la necesidad de un modelo jurídico. *Instituto Español de Estudios Estratégicos*, (6), pp 1-18.

³ GONZÁLES, V. (2023). *Regulación del delito sexual virtual “Grooming (online o child)” e implementación de inteligencia artificial como posible estrategia para contrarrestar esta figura delictiva en Colombia*. [Tesis de maestría, Universidad de los Andes]. Repositorio Institucional de la Universidad de los Andes. <https://hdl.handle.net/1992/73421>.

Aunado a este panorama, las agendas gubernamentales se encuentran notoriamente influenciadas; puesto que, los Estados requieren fortalecerse ante las crecientes amenazas y propiciar un entorno digital fundado en la confianza y seguridad⁴.

ii. Ciberdelincuencia y violencia digital

Hasta el momento se ha evidenciado que el ciberespacio refleja un marco social que excede las categorías jurídicas tradicionales, denotando la necesidad de replantear el marco regulatorio para adaptarlo a las nuevas formas de interacción.

La ciberdelincuencia circunscribe tanto a los delitos comunes, cuya ejecución se apoya de medios informáticos, como a los delitos informáticos, cuya finalidad es atacar a una red informática o un dispositivo⁵. No toda conducta realizada empleando un instrumento tecnológico es un delito informático⁶. Uno de los criterios para dicha clasificación radica en la necesidad del medio informático para su ejecución.⁷

En vista de lo señalado, la criminalidad informática yace como una de las amenazas más generalizadas actualmente, se extiende a miles de instituciones, empresas y demás sectores de la sociedad⁸. En particular, las amenazas de carácter sexual son manifestación de ciberviolencia, nueva modalidad de perjuicio a través de las tecnologías de la información⁹.

⁴ MORÓN, I. (2021). Riesgos que genera el ciberespacio para los derechos fundamentales. *Revista penal México*, (18), pp. 185-200.

⁵ PEÑA, D. (2023). Ciberdelitos y criminalidad informática: Rol de la prevención en la expansión de la ciberdelincuencia. *Informática y Derecho: Revista Iberoamericana de Derecho Informático (segunda época)*, (13), pp. 57-72.

⁶ VILLAVICENCIO, F. (2014). Delitos Informáticos. *Ius et Veritas*, (49), pp. 284-304

⁷ MAZUELOS, J. (2007). Modelos de imputación en el Derecho penal informático. *Derecho Penal y Criminología*, *Derecho Penal y Criminología* 28, (85), pp. 37-54.

⁸ TÁVORA, M. (2022). *Vigilancia e investigación policial en el ciberespacio: aspectos procesales del ciberpatrullaje* [Tesis doctoral, Universidad de Sevilla]. Repositorio institucional de la Universidad de Sevilla. <https://dialnet.unirioja.es/servlet/tesis?codigo=309409>

⁹ DOMÍNGUEZ, R. (2023). La ciberviolencia en la actualidad: la pantalla como arma letal contra la integridad personal. Dilemas contemporáneos: Educación, Política y Valores. <https://doi.org/10.46377/dilemas.v11i1.3770>.

La violencia digital, ciberviolencia o violencia a través del uso de las TIC puede definirse como “aquella conducta intencionada con la que se causa un daño o un perjuicio a través de las Tecnologías de la Información y de la Comunicación, principalmente el teléfono móvil e Internet”¹⁰. Esta nueva modalidad es ampliamente visualizada en el abuso de las redes sociales, en donde la privacidad se involucra de manera significativa, especialmente, para generar contextos de vulnerabilidad digital¹¹.

Sumado a ello, la VIOLENCIA DIGITAL tiene particularidades que la transforman en un área de especial atención. Entre ellas, se obstaculiza la identificación del agresor, lo cual impide una sanción efectiva. Asimismo, este ambiente permite la preminencia del maltrato en cualquier espacio temporal y, principalmente, goza de sutileza desde la vista de terceros no involucrados directamente, lo cual impide una persecución eficaz¹².

A. Particularidades de los delitos informáticos contra la indemnidad y libertad sexual

La violencia sexual ejercida a través de medios informáticos encuentra diversas manifestaciones, las cuales no discriminan grupos etarios; no obstante, los menores de edad son la población más vulnerable ante estas conductas.

Por un lado, el sexting es una práctica sexual que implica la difusión de imágenes o vídeos de contenido íntimo a través de un ordenador, siendo pasible de sanción penal en los casos donde no haya consentimiento de la víctima¹³. Una técnica utilizada para ello es el craking, donde el agente roba el contenido mediante el acceso

¹⁰ GARCÍA, D. et al. (2011). Violencia a través de las tecnologías de la información y la comunicación en estudiantes de secundaria. *Anales de Psicología / Annals of Psychology* 27, (1), pp. 221-31.

¹¹ VERDEJO, M. (2015). *Ciberacoso y violencia de género en redes sociales: análisis y herramientas de prevención*. Universidad Internacional de Andalucía.

¹² GARCÍA, D. et al. (2011). Violencia a través de las tecnologías de la información y la comunicación en estudiantes de secundaria. *Anales de Psicología / Annals of Psychology* 27, (1), pp. 221-31.

¹³ PALOP, M. (2019). *Protección Jurídica de Menores Víctimas de Violencia de Género a Través de Internet Vulnerabilidad de la Menor en sus Relaciones de Pareja*. Ciberacoso y Derecho al Olvido.

al dispositivo electrónico de su víctima, con la finalidad de difundir o ceder las imágenes sin su consentimiento.

Si bien el sexting puede realizarse dentro de los márgenes de la licitud, habrá situaciones donde se convierta en el insumo para una sextorsión o pornovenganza¹⁴. Este comportamiento es una forma de amenaza, extorsión y chantaje sexual realizado por internet con la finalidad de doblegar la voluntad de la víctima mediante la amenaza de difundir su imagen o vídeo íntimo.

Otra forma de violencia sexual digital es el cyberflashing o ciber exhibicionismo que consiste en el envío de imágenes obscenas a una persona desconocida por la red, sin que se lo haya solicitado. Igualmente, el flaming es aquella conducta dirigida a provocar al receptor a través de mensajes ofensivos e intimidantes¹⁵.

Uno de los fenómenos de trascendencia internacional es el *child grooming*, el cual abarca las estrategias que una persona ejerce para ganarse la confianza de un menor de edad y aprovecharse de su vulnerabilidad, buscando obtener contenido de índole sexual y, en los peores casos, solicitar un encuentro con la víctima¹⁶. Este conjunto de estrategias malintencionadas incluye multiplicidad de actividades de índole sexual, que puede incluir conversaciones, emisión de imágenes y, en lo más severo, la concretización de relaciones sexuales virtuales a través de la webcam o un encuentro físico.

Por ello, se reconoce como un proceso gradual de alta complejidad, cuya efectividad suele depender del enamoramiento o seducción que consigue el groomer respecto del menor de edad. Así, su desarrollo ha sido delimitado en cinco rasgos esenciales: 1) técnicas

¹⁴ Denominado *porn revenge* en la doctrina norteamericana para referirse a estos casos.

¹⁵ DOMÍNGUEZ, R. (2023). La ciberviolencia en la actualidad: la pantalla como arma letal contra la integridad personal. Dilemas contemporáneos: Educación, Política y Valores. <https://doi.org/10.46377/dilemas.v11i1.3770>.

¹⁶ ESPINOSA, J. (2019). Ciberdelincuencia. Aproximación criminológica de los delitos en la red. *La Razón histórica: revista hispanoamericana de historia de las ideas políticas y sociales*, (44), pp. 153-73.

de manipulación y control; 2) dirigido hacia un sujeto vulnerable; 3) realizado en diversas relaciones inter-personales; 4) generar confianza o normalizar la conducta sexual; y 5) busca facilitar una exposición prohibida¹⁷.

En la preparación de este contexto delictivo, el sujeto activo responde a distintas motivaciones; no obstante, son dos las vías más evidentes. En primer lugar, la desensibilización frente a la pornografía adulta, lo cual provoca la búsqueda de comunicaciones sexuales con menores de edad. En segundo lugar, la concretización de fantasías a través de la pantalla, evadiendo el mundo real¹⁸.

Pero ¿qué convierte a estas conductas en un reto para el derecho penal? En buena cuenta, la inmediatez que brinda la virtualidad para que el abusador contacte niños, niñas y adolescentes es incomparable a sus posibilidades en el mundo real. Este espacio le permite estudiar a su víctima y recaudar toda la información que le resulte útil¹⁹. Asimismo, la desterritorialización facilita que el victimario agrede a quienes encuentre vulnerables en el universo digital, sin mayores limitaciones. Esto se vincula con la facilidad de encarnar diferentes perfiles, puesto que, la virtualidad incrementa la dificultad para distinguir al abusador y facilita su interacción con sus víctimas²⁰.

Todo ello sugiere que, las agresiones sexuales se magnifican en este universo, donde el sujeto activo se sirve de las herramientas digitales para facilitar sus objetivos nocivos y gozar de impunidad.

¹⁷ McAlinden, A. (2013). "Grooming" and the Sexual Abuse of Children: Implications for Sex Offender Assessment, Treatment and Management. *Sexual Offender Treatment* 8, (1).

¹⁸ WEFERS, S. et al. (2021). Understanding and Detering Online Child Grooming: A Qualitative Study. *Sexual Offending: Theory, Research, and Prevention* 19, pp. 1-27. <https://doi.org/10.5964/sotrap.13147>.

¹⁹ MIRÓ, F. (2012). El cibercrimen: fenomenología y criminología de la delincuencia en el ciberespacio. *Ediciones Jurídicas y Sociales*. <https://dialnet.unirioja.es/servlet/libro?codigo=756351>.

²⁰ CRUZ, L. (2021). El "Child Grooming" y regulación del delito sexual virtual contra niños, niñas y adolescentes en Colombia. *Derecho Penal y Criminología*, *Derecho Penal y Criminología* 42, (113), pp. 43-96.

De ahí que, el Convenio de Budapest y el conjunto de recomendaciones internacionales ha exhortado a los países a tipificar las diversas conductas que recaen sobre el abuso de menores de edad²¹ en el marco de las nuevas tecnologías.

En esta línea, el uso de sistemas de inteligencia artificial y el análisis predictivo se erige como una medida necesaria para prevenir estos delitos. A través de la policía predictiva, la implementación de algoritmos permite el procesamiento de grandes volúmenes de datos que detectan patrones de riesgo y a posibles agresores. No obstante, existen ciertos riesgos en su desarrollo, lo cual decantaría en falsos positivos y una transgresión injustificada de la igualdad. Por este motivo, el marco normativo internacional se ha adelantado en su regulación.

iii. Regulación normativa sobre el uso de la Inteligencia artificial

La regulación en materia de inteligencia artificial no se ha desarrollado de manera significativa, sin embargo, en los últimos años se tiene esperanza de una evolución continua en la preocupación por este asunto de tanta relevancia, toda vez que involucra una limitación o transgresión sutil de los derechos humanos.

A. Internacional

En primer lugar, se debe enfatizar en los esfuerzos que la Unión Europea (UE) está realizando para elaborar una ley sobre la conducción de la inteligencia artificial, a través de una clasificación de los riesgos y otras normas específicas contextualizadas a la complejidad digital.

Para ello, en el año precedente la UE ha aprobado el Reglamento sobre Inteligencia Artificial, el cual establece normas para regular el desarrollo y uso de sistemas de IA, exhortando que se aplique un enfoque precautorio centrado en el respeto de los derechos fundamentales. Por lo expuesto, se ha realizado una clasificación de los sistemas por el nivel de riesgo, siendo los de riesgo alto aquellos vinculados con derechos como salud, seguridad y otros conexos.

²¹ *Ídem.*

Asimismo, en este documento se especifica el tratamiento que debe seguirse con respecto a la protección de datos personales, señalando que debe evitarse la vigilancia masiva y un uso arbitrario de la identificación biométrica en áreas públicas. Sumado a ello, se destaca la necesidad de implementar el uso de estas tecnologías con transparencia y garantizar la supervisión humana, de manera que se exige que estos sistemas sean supervisables.

En la región americana, Chile busca regular el proyecto de ley sobre sistemas de inteligencia artificial, robótica y tecnologías conexas, considerando la clasificación realizada por la Unión Europea, toda vez que prevé riesgos inaceptables y sistemas de nivel elevado de riesgo. En este país se puede visualizar una evolución significativa en los marcos regulatorios para el uso de la IA, lo cual se hizo visible desde la emisión primigenia de la Política Nacional de Inteligencia Artificial de 2021.

Entre los productos legislativos dirigidos a esta finalidad se encuentran la Ley Marco sobre Ciberseguridad y el Proyecto de Ley sobre Delitos Informáticos que abordan la regulación de la IA en los sistemas de seguridad y en relación con la protección de datos personales. Lo dicho resalta que, la actualización legislativa en Chile se guía por la necesidad urgente de armonizar el desarrollo tecnológico con los derechos fundamentales. Destacando principios de transparencia, no discriminación y rendición de cuentas en el uso de estas nuevas herramientas, alineándose a lo establecido a nivel internacional por la OCDE y la UNESCO²².

Así también, en la experiencia argentina se ha hecho uso de los estándares internacionales en base a principios éticos recomendados por los organismos internacionales anteriormente citados. Entre las principales acciones del Estado argentino, se puede mencionar la inclusión de la IA en la Agenda Digital Argentina 2020 y la elaboración de los Principios Éticos para la IA del 2021. Estos documentos adscriben la equidad, no discriminación, seguridad

²² REMESEIRO, R. (2025). La propuesta de Regulación de la Inteligencia Artificial en Chile y el Reglamento Europeo de Inteligencia Artificial, ¿un caso de efecto Bruselas? *IDP. Revista de Internet, Derecho y Política*, (42), pp. 1-12. <https://doi.org/10.7238/idp.v0i42.431597>.

y responsabilidad en el manejo de las herramientas inteligentes, enfocándose en la prevención.

La trascendencia de estos avances resalta la exigencia de una regulación especial centrada en los riesgos de discriminación algorítmica, vigilancia masiva, decisionismo automatizado y el quebrantamiento general de la privacidad en aras de otros intereses colectivos. Frente a esto, Argentina incorpora un enfoque que regula la IA por su utilidad para el ser humano, lo cual permite priorizar los elementos fundantes de un Estado de Derecho y fortalecer la garantía de los derechos fundamentales sin desconocer la innovación tecnológica²³.

Otro país que se encuentra en proceso de construcción de un marco legal y ético en la utilización de la IA es México, centrándose en la construcción de políticas públicas y participación de organismos especializados. Uno de los avances más destacados es la creación de una Estrategia Nacional de Inteligencia Artificial en 2018, la cual propuso el desarrollo inclusivo, ético y sostenible de las nuevas tecnologías, sin eludir los principios contenidos en la OCDE y la UNESCO.

Pese a todos los esfuerzos, aún se identifican retos importantes para traducir las iniciativas en un marco regulatorio específico sobre el uso de la IA. Aún persiste la necesidad de garantizar la supervisión humana sobre los sistemas inteligentes, en especial dentro de los contextos relacionados a la justicia, la seguridad pública y otros servicios esenciales²⁴.

B. Nacional

El 5 de julio del 2023 se promulgó la Ley N.º 31814, la cual buscó impulsar el desarrollo económico y social permitiendo el uso de

²³ VERCELLI, A. (2024). Regulaciones e inteligencias artificiales en Argentina. *Inmediaciones de la Comunicación* 19, (1), pp. 52-74. <https://doi.org/10.18861/ic.2024.19.1.3549>.

²⁴ MEDINA, M. y TORRES, T. (2025). Regulación de la Inteligencia Artificial: Desafíos para los Derechos Humanos en México. *RIDE Revista Iberoamericana para la Investigación y el Desarrollo Educativo* 15, (30). <https://doi.org/10.23913/ride.v15i30.2291>.

tecnologías y, en específico, la inteligencia artificial, la cual define como una tecnología emergente que tiene un propósito general: potenciar el bienestar humano.

Entre los principios fundamentales que se desarrollan en este instrumento se verifica un enfoque fundado en la identificación del nivel de riesgo, tal como se realizó en el reglamento emitido por la Unión Europea (UE). Igualmente, mediante la pluralidad en la participación se busca que los actores públicos colaboren con los entes privados para asegurar una visión correcta e inclusiva. Esto último encuentra vinculatoriedad en el ejercicio ético y acorde a los derechos fundamentales, toda vez que se busca preservar la privacidad en su uso.

Pese a ello, su reglamentación no sigue la clasificación originalmente planteada por la UE; puesto que, no se han contemplado otros supuestos de riesgo inaceptable como los siguientes:

- Sistemas de evaluación de riesgos y elaboración de perfiles predictivos de delincuencia.
- Sistemas de IA que creen o amplíen bases de datos de reconocimiento facial.
- Sistemas de IA de identificación biométrica remota en tiempo real en espacios públicos

Estas consideraciones son importantes para el presente trabajo de investigación, ya que los presupuestos ignorados en la reglamentación de la ley N.º 31814 habilitan el uso indistinto de sistemas de inteligencia artificial para prevenir o investigar delitos en el contexto digital.

Esta ley aún requiere mejoras para garantizar los marcos de acción que tienen las personas ante riesgos que pudieran lesionar sus derechos fundamentales entre los cuales están vinculadas al acceso, transparencia de la información y protección de datos personales, simplificación de procesos administrativos y otras sobre seguridad informática y gestión de las tecnologías de la información²⁵. Sin

²⁵ FLOR, A. (s. f.) La vulneración de los derechos fundamentales a través de la inteligencia artificial. *SAPIENTIA & IUSTITIA*, (11), pp. 5-24. <https://doi.org/10.35626/sapientia.11.6.113>.

embargo, constituye un avance notorio en la regulación de la IA dentro de la jurisdicción peruana.

iv. Los sistemas inteligentes creados para la prevención y persecución delictiva

La inteligencia artificial (IA) pretende imitar en la mayor medida posible los procesos cognitivos humanos, de tal manera que su aprendizaje busca asemejarse a la percepción y captación de una sumatoria de experiencias. En este sentido, la IA aplicada a la prevención delictiva se basa en el aprendizaje automático o computacional, lo cual permite una construcción de decisiones rápidas en base a contenido preexistente a su operatividad.

En este acápite expondremos algunos de estos sistemas predictivos. Por un lado, HunchLab se centra en identificar áreas predictivas para la criminalidad, lo cual permite que el sistema policial tenga un mejor margen de acción y ostente precisión en su función preventiva. Igualmente, a través del uso de Strategic Subject List se realiza una clasificación de las personas de acuerdo con su historial delictivo, permitiendo que se les asigne un nivel de peligrosidad.

Por otra parte, mediante la implementación de Clearview se permite la identificación automática de un agente delictivo por el reconocimiento facial realizado en base a fotografías disponibles en la red²⁶. Estos sistemas de inteligencia artificial carecen de una visión enfocada en agresiones de carácter sexual, pero son igualmente relevantes de hacer mención.

En el ámbito específico del child grooming, Child Safe AI dirige su funcionalidad a la recopilación de índices de explotación sexual reflejados en los diálogos o fotos emitidos por los usuarios de internet. En el mismo sentido, Spotlight obtiene información de los sitios web que estén vinculados con el tráfico y abuso infantil, donde identifica

²⁶ RODRÍGUEZ, S., MALDONADO, L. (2024). Reflexión sobre el uso de la inteligencia artificial en la investigación penal en el Ecuador-análisis de su aplicabilidad en el derecho comparado. *Polo del Conocimiento* 9, (2). <https://doi.org/10.23857/pc.v9i2.6584>.

a las posibles víctimas, sus agresores y otras conductas dirigidas a esta finalidad delictuosa, esta resulta en una herramienta similar a la Tecnología de IA del Instituto Interregional de las Naciones Unidas para la investigación, el Crimen y la Justicia²⁷.

A su vez, destaca CATT (Chat Analysis Triage Tool), un algoritmo creado por el Instituto Politécnico de la Universidad de Purdue (Indiana), concebido como una herramienta basada en el procesamiento del lenguaje natural. Su finalidad es contrastar conversaciones en línea entre los menores y sus depredadores sexuales para estimar un nivel de riesgo y calcular la probabilidad de que el interlocutor intente concretar un encuentro físico con la víctima.

Por otra parte, una ONG holandesa creó Sweetie, una niña virtual que interactúa con presuntos pederastas en tiempo real, con el objetivo de recabar la información necesaria para su identificación y eventual enjuiciamiento. Su eficacia fue tal que consiguió atraer a más de mil agresores sexuales por internet²⁸.

Lo que se cuestiona de los sistemas de prevención delictiva es que sus inferencias se sustentan en una base de datos que no está del todo verificada y, en consecuencia, puede dar lugar a respuestas sesgadas. Como se ha expuesto, los sistemas son de diversa índole – análisis de texto, procesamiento del lenguaje, etc. – cada uno con sus propios sesgos. Conviene señalar, estos pueden ser de diferente naturaleza: de presentación, de filtro, de muestreo, histórico, de interacción, entre otros igualmente importantes de estudiar²⁹.

Esto se convierte en un gran problema cuando afecta las decisiones policiales y jurisdiccionales, ya que una predicción sesgada puede orientar un despliegue innecesario de diligencias. Asimismo, si la base de datos contiene información específica de ciertos perfiles (idioma,

27 GONZÁLES, V. (2023). *Regulación del delito sexual virtual "Grooming (online o child)" e implementación de inteligencia artificial como posible estrategia para contrarrestar esta figura delictiva en Colombia*. [Tesis de maestría, Universidad de los Andes]. Repositorio Institucional de la Universidad de los Andes. <https://hdl.handle.net/1992/73421>.

28 Noticia: (4 de noviembre de 2013). Niña virtual "atrapa" a más de mil pedófilos, *BBC News Mundo*. https://www.bbc.com/mundo/ultimas_noticias/2013/11/131104_ultnot_paidofilia_virtual_wbm

29 LLANO, F. et al. (2022). *Inteligencia artificial y Filosofía del derecho*. Laborum,

género, origen geográfico, etc.) el sistema tenderá a reproducir dichas características en su análisis de datos.

En el Perú, la Policía Nacional ha elaborado investigaciones sobre las implicancias éticas y legales en torno a la utilidad de la IA y otras herramientas tecnológicas dentro de las operaciones policiales. Un reciente artículo de la Unidad de Posgrado de la PNP concluye que, la ausencia de marcos normativos sólidos y efectivos en la supervisión de la implementación de IA, drones y sistemas biométricos genera riesgos significativos para los derechos fundamentales, dando lugar a prácticas desproporcionadas y arbitrarias³⁰.

Por estos motivos, en la actualidad se contempla la necesidad de estructurar un conjunto de normas que regulen el uso de la tecnología y la inteligencia artificial, en tanto convergen con derechos fundamentales, pero es inevitable su evolución y apropiación a la cotidianeidad.

v. Ventajas y desventajas del uso de los sistemas inteligentes para la prevención delictiva

La principal ventaja radica en su capacidad para procesar y analizar grandes volúmenes de datos con una rapidez y precisión imposibles para la naturaleza humana. Esto permite identificar patrones espaciotemporales y focalizar las fuerzas policiales en los lugares y momentos de mayor probabilidad delictiva (hot-spot policing)³¹. De este modo, herramientas como el reconocimiento biométrico, procesamiento del lenguaje y otros facilitan la evaluación de un sin número de información dispersa.

Otra ventaja de la IA es la personalización de estrategias preventivas y la mejora en la objetividad de las decisiones judiciales. El empleo de la predicción automatizada para calcular índices de reincidencia o peligrosidad hace posible ajustar las decisiones a la realidad de cada caso. Para lograr dicha efectividad, se proponen ciertos filtros, como es exigir que los datos sean ricos en su diversidad, evitando que la representación de ciertos grupos perjudique la predicción neutral.

30 CHAVARRY, L. et al. (2025). Uso de inteligencia artificial, drones y biometría en las operaciones policiales: una revisión sistemática de sus implicaciones éticas y legales. *Revista Espogra PNP*, 4 (2). <https://doi.org/10.59956/espograpnpv4n2.4>.

31 LUNARDI, et al. (2025). *Digital Transformation and Governance in the Judiciary*. Instituto Jurídico da Faculdade de Direito da Universidade de Coimbra

Esto refiere que, la utilidad será mayor cuando los sistemas incorporen adecuadamente las realidades socioeconómicas, culturales y territoriales en su programación.

Entre las desventajas más significativas se encuentra el riesgo de los sesgos algorítmicos, ya que su implementan depende de las preconcepciones que mantenga su programador. Por esta razón, si los datos reflejan patrones discriminatorios, la IA simplemente amplificará su alcance. Igualmente, el uso de tecnologías como el reconocimiento biométrico remoto, la geolocalización masiva o el rastreo plantea severos cuestionamientos por el tratamiento de información personal sin autorización.

Un claro ejemplo se verificó en un caso estadounidense, donde un ciudadano fue condenado a seis años de pena privativa de libertad, cuyo quantum fue determinado por un software que analiza la reincidencia y permite influir en el marco punitivo³². Dicho sistema fue cuestionado por The Disparate Impact of Criminal Justice Risk Assessment en 2016, pues se comprobó que contaba con algoritmos fundados en categorías raciales, específicamente, personas afrodescendientes a quienes identificaba como de “alto riesgo”.

La operación Sweetie fue la creación de un avatar con características de una niña filipina, con el fin de identificar a los agresores de menores en la red. Este sistema funcionaba de manera automática y con una simulación humana destacable, donde la IA actuaba como una niña y respondía los mensajes adultos que le llegaban a las distintas plataformas en las que interactuaba. Toda la información recolectada era inmediatamente enviada a las autoridades competentes para iniciar investigaciones.

Pese a lo beneficioso que pueda imaginarse, el proyecto generó ciertas discusiones teóricas y éticas, debido a que la recolección de información se realizaba indiscriminadamente, es decir, los datos personales de todos los posibles “sospechosos” estaban en la nube y eran manejados por los organizadores del proyecto, lo cual a primera vista transgrede la privacidad y el uso de datos personales.

En el marco de la actividad policial, se pueden mencionar otros problemas

³² VESTRI, G. (2021). La inteligencia artificial ante el desafío de la transparencia algorítmica: Una aproximación desde la perspectiva jurídico-administrativa. *Revista Aragonesa de Administración Pública*, (56), pp. 368-98.

en los sistemas de IA como la falta de transparencia para la toma de decisiones en la investigación, la opacidad de los algoritmos y su escasa supervisión, lo cual puede dar lugar a trabajar sobre desigualdades preexistentes³³.

La ausencia de regulación sobre estos sistemas se traducirá en decisiones injustas o investigaciones arbitrarias. Por este motivo, los algoritmos y la automatización en la toma de decisiones es un tema de importante atención, toda vez que, los resultados que generan pueden repercutir irremediabilmente en los derechos fundamentales de las personas, no solo el derecho a la igualdad en su dimensión de no discriminación, incluso el derecho a la misma libertad si se empezara a validar su uso y confianza con total plenitud³⁴.

A. Impacto de los sesgos algorítmicos en el derecho a la igualdad

a. Contenido del derecho a la igualdad

La Real Academia Española refiere que el término igualdad alude al principio que reconoce a todos los ciudadanos capacidad para los mismos derechos. No es una concepción alejada de la realidad, no obstante, implica mucho más que considerar a todos como titulares de protección.

En la interpretación constitucional sistemática, algunos derechos presentan una triple identidad: son simultáneamente derechos fundamentales, principios y valores superiores del ordenamiento jurídico. Así, los valores son el fundamento axiológico vinculado a la finalidad última del sistema, los principios son mandatos dirigidos al poder público e incluso a particulares para garantizar ciertos deberes, y los derechos constituyen posiciones subjetivas de ventaja que corresponden a un titular frente a un obligado, implicando la existencia de una prestación exigible.

³³ CHAVARRY, L. et al. (2025). Uso de inteligencia artificial, drones y biometría en las operaciones policiales: una revisión sistemática de sus implicaciones éticas y legales. *Revista Escpogra PNP*, 4 (2). <https://doi.org/10.59956/escpograpnpv4n2.4>.

³⁴ TENORIO, G. (2021). El derecho a una vida libre de algoritmos. *Revista IUS* 15, (48), pp.115-35. <https://doi.org/10.35487/rius.v15i48.2021.708>.

Dicha transversalidad ha sido reconocida para el derecho a la igualdad, reflejando la trascendencia que ostenta dentro del ordenamiento jurídico peruano. En este sentido, la igualdad como principio permite limitar la función legislativa, toda vez que, se constituye como un punto de interpretación³⁵. Esto se condice con el Exp. N.º 0045-2004-PI/TC, en el cual el Tribunal Constitucional ha declarado que este derecho-principio se vincula con la proyección de todo el orden normativo.

En cambio, cuando nos referimos al derecho a la igualdad en su funcionalidad como derecho fundamental implica realizar un análisis de su estructura triádica. Esta particularidad circunscribe tres elementos: una disposición normativa (texto constitucional), norma (interpretación del texto) y una posición iusfundamental (titular-obligado-mandato). Esta última implica la existencia de una relación jurídica, la cual puede plantearse entre individuos o, en otras oportunidades, entre el Estado y los particulares³⁶.

En concordancia, el artículo 2 inciso 2 de la Carta Magna establece que todos los peruanos tienen derecho a la igualdad ante la ley y a no ser discriminado por motivos de raza, religión, opinión socioeconómica u otro motivo análogo. Siendo así, el contenido iusfundamental protegido abarca el derecho a la igualdad en el contenido y aplicación de la ley, derecho a un trato especial cuando se requiera y el derecho a no ser discriminado.

En mayor atención, el derecho a no ser discriminado debe entenderse como una posición iusfundamental de inviolabilidad o inmunidad, toda vez que se configura como una regla inquebrantable. Todo ciudadano tiene el derecho frente al Estado y los particulares de que no se le diferencie por razones

³⁵ LANDA, C. (2021). El derecho fundamental a la igualdad y no discriminación en la jurisprudencia del Tribunal Constitucional del Perú. *Estudios constitucionales* 19, (2), pp. 71-101. <https://doi.org/10.4067/S0718-52002021000200071>.

³⁶ BERNAL, C. (2014). *El principio de proporcionalidad y los derechos fundamentales: El principio de proporcionalidad como criterio para determinar el contenido de los derechos fundamentales vinculantes para el Legislador*. Universidad Externado.

que forman parte de su dignidad como ser humano, a menos que haya una razón constitucionalmente relevante que lo justifique.

De este modo, se proscribe la discriminación recaída sobre “categorías sospechosas”: características inherentes al ser humano (involuntarias) como son la raza, el sexo, idioma, condición económica, orientación sexual, etc. y las posiciones voluntarias que forman parte de la personalidad de un individuo, ya sea el credo, opinión o filiación política.

Cabe precisar que no todo trato desigual es discriminatorio, esto es, si se encuentran motivos objetivos y razonables para la diferenciación, el trato será constitucionalmente tolerable³⁷. El derecho a no ser discriminado coloca a la persona en una posición de tutela especial, donde no debe verse afectado o perjudicado, tratándose de una protección absoluta sobre su esfera individual. Por ende, esta posición iusfundamental no admite una garantía condicionada o sopesada con otros bienes jurídicos³⁸.

- b. Entonces, ¿cómo afectan los algoritmos al contenido del derecho a la igualdad?

Los algoritmos son el conjunto de procedimientos generalizados que se dedican a convertir entradas de datos caóticos en salidas comprensibles mediante una serie de reglas lógicas³⁹. Así parece que la toma de decisiones basada en algoritmos goza de neutralidad y objetividad, pero no es del todo cierto. Para su operatividad se puede valer de desinformación, racismo o prejuicios señalados por su creador⁴⁰.

Si los algoritmos se entrenan con datos sociales sin garantizar su objetividad, pueden generar resultados que reflejen distinciones

³⁷ Sentencia del Tribunal Constitucional 02974-2010-AA, fundamento jurídico 7.

³⁸ SOSA, J. (2024). *El derecho a la igualdad y no discriminación en la jurisprudencia del Tribunal Constitucional y de la Corte IDH*. Palestra.

³⁹ KOED, A. et al. (2016). Big Data: Issues for an International Political Sociology of Data Practices 1. *International Political Sociology*, 10 (3), pp. 275-96. <https://doi.org/10.1093/ips/olw010>.

⁴⁰ LARRONDO, F. (2020). *Inteligencia artificial y derecho*. Hammurabi.

arbitrarias entre distintos grupos de personas. Por ejemplo, el reconocimiento digital que realiza un sistema de inteligencia artificial podría enfocarse en ciertos perfiles que se adecúen a las características tradicionalmente vinculadas con la criminalidad.

Más allá de ser herramientas, los algoritmos constituyen estabilizadores de confianza y garantías fundadas en el mito de la imparcialidad. Sin embargo, no debe ignorarse que se crean con propósitos claros. Determinan preferencias de comportamiento y estructuras para identificar, ordenar y clasificar a las personas⁴¹.

En el marco de la prevención delictiva, uno de los impactos más evidentes de estos sesgos es la discriminación racial y socioeconómica. En la medida que los sistemas de IA están entrenados por personas con sus propias cargas morales incluyen datos históricos que estigmatizan a ciertos grupos. Esto se puede manifestar en aquellos sistemas que agrupan a determinadas etnias como grupos de “alto riesgo” y, en consecuencia, provocan detenciones y cuestionamiento infundados⁴².

Sumado a ello, se ha reconocido el “efecto contagio” delictivo en el uso de estos sistemas de IA, cuyo razonamiento radica en asumir que los delitos futuros serán igualmente ejecutados. Esto significa que, si en un inicio las inferencias brindadas por los algoritmos se dirigieron a señalar determinados perfiles como posibles sospechosos, el mecanismo continuará enfocándose en dichos grupos o en el mismo *modus operandi*. Si no prevé mayores escenarios en la fase de programación, continuará perpetuando la discriminación y eludiendo otras prácticas o personas que se alejen del marco lógico con el que fue creado.

Esto es particularmente relevante en sistemas como CATT, que se enfoca en analizar las interacciones en línea. Si su entrenamiento se ha puntualizado con determinadas pautas culturales, es posible que detecte casos de grooming con mayor precisión en ciertas interacciones y omita otras. Igualmente, con Sweetie, pues al operar como un único perfil digital genera un

⁴¹ KITCHIN, R. (2018). *Thinking critically about and researching algorithms*. Routledge.

⁴² *Ídem*.

sesgo incluso desfavorable para la finalidad preventiva: sesgo selectivo que excluye el perfil de los depredadores sexuales que están en busca de menores de edad con otras características físicas.

Pese a estas falencias, los Estados no pueden quedarse con los brazos cruzados. Si los índices de las agresiones sexuales en línea – o la criminalidad en general – señalan una emergencia, es innegable que se deben implementar medidas lo suficientemente efectivas para contrarrestar estas conductas.

Dado que el derecho a la igualdad y no discriminación posee un contenido de indemnidad frente a diferenciaciones injustificadas, se debe optar por una manera de legitimar el uso de estos sistemas predictivos sin anular el contenido constitucionalmente protegido.

Sobre ello, si se privilegiara únicamente la seguridad pública, se aceptaría sin más la implementación de los sistemas predictivos inteligentes, pese a los evidentes sesgos algorítmicos que presentan. Mientras que, si solo protegemos la igualdad y no discriminación, se impide potenciar la capacidad del Estado para prevenir delitos con alta complejidad, como en estos espacios digitales. Al respecto, uno de los métodos de resolución de conflictos entre derechos fundamentales es el criterio de concordancia práctica, el cual permite la coexistencia de los intereses en conflicto, conservando su máxima eficacia posible⁴³.

A partir de ello, para optimizar el derecho a la igualdad y garantizar la seguridad pública en el espacio digital, se hace necesario introducir una serie de mecanismos que permitan valerse de la utilidad de la inteligencia artificial, sin sacrificar el derecho a la igualdad y no discriminación.

⁴³ RONDON, B. (2024). La concordancia práctica: una relectura a los planteamientos de Konrad Hesse. *Cuestiones constitucionales*. <https://doi.org/10.22201/ijj.24484881e.2024.51.17960>.

B. Medidas para reducir la incidencia de los sesgos algorítmicos

En primer lugar, resaltamos que la naturaleza de los delitos ejecutados en redes informáticas requiere un tratamiento especializado y contextualizado. Con mayor énfasis, la prevención e investigación de las agresiones sexuales en esta nueva realidad es un tema de amplia preocupación.

No obstante, el accionar de los agentes encargados de la prevención e investigación delictiva requiere acogerse a la protección de los derechos constitucionalmente reconocidos. El Estado cuenta con un amplio margen de acción y un poderío que requiere limitaciones precisas y reforzadas, en especial, cuando se trata de implementar medidas automatizadas.

Los ejemplos descritos anteriormente, evidencian el riesgo latente en la operatividad de estos sistemas de inteligencia artificial, su capacidad de predicción se encuentra condicionada a su base de datos, la cual existe sin una regulación especial para identificar el contenido potencialmente lesivo hacia los derechos fundamentales. Por ello, algunos autores los denominan “cajas negras” que no consiguen explicar de qué modo han tomado sus decisiones y eso complica detectar o subsanar los elementos de discriminación que hayan empleado⁴⁴.

No se pretende condenar el uso de sistemas basados en IA, por el contrario, se comprende que se han convertido en una herramienta de amplia utilidad para afrontar la criminalidad. Lo que se busca es exponer la necesidad de una regulación ajustada a su realidad para impedir la arbitrariedad en su uso, atenuar falta de certeza y la comprobada influencia de sesgos algorítmicos.

Como se reconoce en un informe adoptado por la Asamblea Parlamentaria del Consejo de Europa (PACE) en 2017, la peligrosidad de la inteligencia artificial exige regular su fase de programación, con el fin de impedir una injerencia injustificada sobre

⁴⁴ ITURMENDI, J. (2023). La discriminación algorítmica y su impacto en la dignidad de la persona y los derechos humanos: Especial referencia a los inmigrantes. *Revista Deusto de Derechos Humanos*, (12), pp. 257-84.

los derechos humanos y evitar las decisiones fundadas en motivos discriminatorios.

En el contexto peruano, el panorama es aún más preocupante, ya que la citada Ley N.º 31814 no ha previsto las falencias de estos mecanismos inteligentes y abre la posibilidad de su empleo en las diferentes actividades de los órganos públicos y privados. Ante ello, la posible implementación de estos sistemas sin la exigencia de criterios de transparencia y corrección de sesgos algorítmicos permite reforzar las prácticas discriminatorias, lo que es peor, de manera sutil y difícilmente identificable.

Para evitar la falta de certeza y la determinación de los sesgos en la funcionalidad de estos sistemas se deben implementar una serie de estrategias preventivas. Por un lado, diversificar los datos, pues la variabilidad en la data aprendida por los algoritmos permitirá que la información delictiva, por ejemplo, no se encasille en determinadas poblaciones que históricamente se han visto vinculadas a la criminalidad por los prejuicios y la segregación. Paralelamente, debe incluirse un universo de contextos y situaciones posibles para dotarla de mayor efectividad.

Asimismo, el funcionamiento de los algoritmos debe ser accesible para entender los criterios que sujetan las inferencias a las que arribe. De este modo, las auditorías realizadas por terceros independientes sería una buena opción para permitir una evaluación exhaustiva de los datos que se manejen en su programación⁴⁵.

Finalmente, la incorporación de principios como la rendición de cuentas, transparencia u otros construye un marco de acción que paralelamente debe ser reforzado con una campaña de concientización sobre los beneficios y las amenazas en el empleo de la inteligencia artificial.

Estas son algunas de las medidas para mitigar el impacto de los sesgos algorítmicos y hacer uso de la IA con la responsabilidad que se requiere. Valerse de su utilidad y practicidad es oportuno, pero en el marco del respeto hacia los derechos fundamentales.

⁴⁵ BUSTELO, J. (2024). El Sesgo algorítmico en la inteligencia artificial. Implicaciones para la seguridad global y la política criminal. *GEOCONFLICTS & INTELLIGENCE: Revista Sobre Seguridad Global y Terrorismo*, 2 (2), pp.183-203.

III. Conclusiones

El panorama no es tan desalentador como parece, una eventual integración de los sistemas de inteligencia artificial a la vigilancia o prevención delictiva requiere de un marco normativo especializado y estructurado para cumplir con su finalidad y no transgredir las garantías constitucionales.

Los sistemas predictivos pueden verse como una herramienta eficaz en la lucha contra la criminalidad, no obstante, la experiencia comparada ha demostrado que existe una tendencia a reproducir sesgos algorítmicos, los cuales se basan en características sociales injustificadas, “categorías sospechosas”.

El aumento constante de la ciberdelincuencia exige al legislador y los encargados de la persecución delictiva adoptar herramientas tecnológicas que optimicen la detección e investigación de estas nuevas formas de criminalidad. En ese sentido, para brindar legitimidad a estas medidas y no incurrir en la lesión del derecho a la igualdad en la toma de decisiones automatizadas, se debe aplicar el criterio de concordancia práctica y optimizar ambos intereses: la seguridad y el derecho a la igualdad.

Para hacer posible esta armonía, es indispensable implementar exigencias previas como la diversificación de datos en su programación, implementación de auditorías independientes y la concientización en el uso ético de estas herramientas. Si bien no se trata de abandonar las oportunidades de su funcionalidad, la incorporación de sistemas de inteligencia artificial en la prevención e investigación de prácticas criminales como el child grooming requieren cautela y previsión en su regulación.



FORSETI